Shelby County Health Department

Health Insurance Portability and Accountability Act (HIPAA)

Security Policy and Procedure Manual

July, 2013 revision

2013

Index

SHELBY COUNTY GOVERNMENT
SHELBY COUNTY HEALTH DEPARTMENT

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
ACCESS TO SYSTEMS CONTAINING PHI

Policy # (HS – 201)	**Supersedes Policy**
Approved By	**Effective Date 04-20-05**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date**

HIPAA Security Language – *Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process or other mechanism.*

SCOPE/APPLICABILITY – This policy applies to all departments that use, disclose or access protected health information for any purposes. This policy's scope includes all protected health information, as described in the Security Rule.

PURPOSE - To issue instructions to all of the Shelby County Health Department's departments and workforce members regarding access controls required for the Shelby County Health Department systems that contain PHI. To provide an adequate level of security to protect the Shelby County Health Department's data and information systems from unauthorized access. This policy defines the rules necessary to achieve this protection and to ensure a secure and reliable operation of the Shelby County Health Department's information systems.

POLICY - Access to the Shelby County Health Department's information system is restricted to its own employees and volunteers of the Shelby County Health Department's, and business associates who have executed a Business Associate Agreement with the Shelby County Health Department.

Users' level of access to the Shelby County Health Department's information systems is granted by their job descriptions and their need to access particular types of information in order to carry out the responsibilities of their specific job position.

The users must meet the following criteria before they are authorized access to information system resources:

- The user has completed orientation and has been assigned specific job responsibilities that require access to certain Shelby County Health Department Information Systems or;
- The user is an employee of a business associate who has an executed Business Associate Agreement on file with the Contracting Department;
- The employee or volunteer has completed the HIPAA Privacy and Security Awareness training class and;

- The Privacy Officer has on file a copy of the Confidentiality Statement and Information System Users Access Notice signed by employee or business associate.

The authority to access or revoke user's privileges rests with the Executive Director, Privacy Officer and Security Officer, or his/her designee.

PROCEDURE

1. Any user (remote or internal) accessing the Shelby County Health Department's networks and systems, must be authenticated. The level of authentication must be appropriate to the data classification and transport medium. Entity authentication includes but is not limited to a requirement of a Unique User Identifier and password.
2. Workstation Access Control System: All workstations used for the Shelby County Health Department's business activity, no matter where they are located, must use an access control system approved by the Shelby County Health Department. In most cases this will involve password-enabled screen-savers with a time-out-after-no-activity feature and a power on password for the CPU. Active workstations are not to be left unattended and accessible for prolonged periods of time. When a user leaves a workstation, that user is expected to properly log out of all applications and networks. Users will be held responsible for all actions taken under their sign-on. Inactive workstations will be reset after a period of inactivity as defined in the Information Technology Services Network Security Policy (typically 15 to 60 minutes). Users will then be required to resubmit their login credentials to continue usage.
3. Disclosure Notice: A notice warning that only those with proper authority should access the system will be displayed initially before signing on to the system. The warning message will make clear that the system is a private network or application and that unauthorized users should disconnect or log off immediately.
4. System Access Controls: Access controls will be applied to all computer-resident information based on its Data Classification to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.
5. Access Approval: System access will not be granted to any user without appropriate approval. The department director or manager is to immediately notify the Security Officer and report all significant changes in end-user duties or employment status for appropriate actions. User access is to be immediately revoked if the individual has been terminated. In addition, user privileges are to be appropriately changed if the user is transferred to a different job.
6. Limiting User Access: The Shelby County Health Department approved access controls, such as user logon, group membership, menus, session managers and other access controls will be used to limit user access to only those network application and functions for which they have been authorized.
7. Need-to-Know: Users will only receive access to the minimum application and privileges required for performance their jobs.
8. Information System User Access Notice: Users who access Shelby County Health Department information systems must sign the Information System User Access Notice prior to issuance of a user-ID. A signature on the Information System

User Access Notice indicates the user understands and agrees to abide by the Shelby County Health Department policies and procedures related to computers and information systems. Periodic confirmations will be required of all systems users.

9. Audit Trials and Logging: Logging and auditing trails are based on the Data Classification of the systems.
    1. Confidential Systems: To the extent possible, access to confidential systems will be logged and audited in a manner that allows the following information to be deduced:
        i. Access time
        ii. User account
        iii. Method of access
        iv. All privileged commands must be traceable to specific user accounts
        v. In addition, logs of all inbound access into the Shelby County Health Department's internal network by systems outside of its defined network perimeter shall be maintained.
        vi. Back-up and Restore: Audit trails for confidential systems shall be backed up and stored in accordance with the Shelby County Health Department back-up and disaster recovery policies. All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons. All logs must be audited on a periodic basis. Audit results should be included in periodic management reports.
        vii. Access for Non-Workforce members: Individuals who are not workforce members, contractors, or business partners must not be granted a user – ID or otherwise be given privileges to use the Shelby County Health Department computer or information systems containing EPHI unless the written approval of the Security Officer has first been obtained before any third party or business partner is given access to this Shelby County Health Department computer or information system, a chain of trust agreement defining the terms and conditions of such access must have been signed by a responsible manager at the third party organization.
        viii. Unauthorized Access: Workforce members are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems. System privileges allowing the modification of "production data" must be restricted to "production" applications.
        ix. Remote Access: As the Shelby County Health Department information system contain PHI and may contain claim information for Medicaid and/or Medicare recipients, remote access must conform at minimum to all statutory requirements including but not limited to the Health Care Finance Administration (HCFA) now known as the Centers for Medicare and Medicaid Services (CMS), and HIPAA. Access must be compliant with the Shelby County Health Department Remote Access Policy.

10. Granting Access in an Emergency

The Privacy Officer has the authority to grant emergency access to users who have not completed HIPAA security awareness training if:

1. The facility declares an emergency or is responding to a natural disaster that makes the management of patient information security secondary to immediate patient care activities.
2. The Privacy Officer determines that granting immediate access is in the best interest of patient care.

If the privacy Office grants emergency access, he/she will review the impact of the emergency access within 24 hours of it being granted and report any potential violation of patient security to the Executive Director.

11. Granting Emergency Access to an Existing User Access Code

In some circumstances it may be necessary for the Privacy Officer to grant emergency access to a user's account without the user's knowledge or permission. The Privacy Officer may grant this emergency access in these situations:

1. The user terminates or resigns without providing the password;
2. The user is seriously ill, unable to communicate, or cannot be reached for a prolonged period;
3. The user has not been in attendance and therefore is assumed to have resigned.

Responsible Parties
Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each health care component. The administrative/management team of each health care component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement
Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment. Additionally, temporaries and volunteers who do not attend training and fail to furnish document of training will not be allowed to furnish services to Shelby County Health Department.

Reference
C. F. R. Sec 164.308 (a)(4)

Shelby County Health Department
Information System User Access Notice

"As an authorized user of the Shelby County Health Department computer systems, I will be given access privileges to Shelby County Health Department, Shelby County, Tennessee State, and Federal government data and computer systems, especially those systems within or accessible by Shelby County Health Department staff including remote systems such as the Internet, to perform the duties of my job. I understand the following policies apply to these data and computer systems:

(1) I will safeguard the passwords and security code(s) given to me. I may use my access security codes in the performance of my official duties. I may not exceed the access authority provided by my security codes. I acknowledge that I am strictly prohibited from disclosing my security code(s) to anyone for any reason except to the facility Information Security Officer (ISO). This includes my family, friends, fellow workers, supervisors, and subordinates.

(2) I acknowledge that I am not to use anyone else's security code(s) to obtain access to the above mentioned computer systems. I understand that I will be held accountable for all work performed or changes made to the system and/or databases under my security code(s) and that I am not to allow anyone else to access a computer system using my security code(s).

(3) I understand that all data to which I may obtain access is and will remain the property of the providing entity. I understand that, as an employee, I have an obligation to protect data and information which the loss, misuse, or unauthorized modification of or unauthorized access to could adversely affect the conduct of Shelby County Health Department or other programs. Further, I am aware that information about individuals, including my own record, is confidential and must be protected by law and regulations from unauthorized disclosure.

(4) I understand that Shelby County Health Department electronic mail is to be used for official government business only. I am not authorized to use electronic mail either for personal messages not related to the performance of my official duties or in lieu of personal telephone calls.

(5) I understand that the ISO and computer staff will monitor the amount, types and contents of Internet access or messages sent by individuals on electronic mail, and that reports may be generated regularly about how Internet access and electronic mail is used by individual employees, including myself.

(6) I understand that improper access to, or unauthorized modification or disclosure of data (obtained through the computer or otherwise) may subject me to the imposition of criminal penalties and/or disciplinary or adverse action, as appropriate, under Shelby County employee conduct regulations. Similarly, if I exceed my computer system access authority or use that authority to engage in conduct outside the scope of my official

duties, I may also be subject to disciplinary or adverse action as appropriate, even criminal prosecution.

(7) I understand that I am not to use my access authority to these computer systems, particularly electronic mail, for any purpose other than performance of my official duties. Specifically, I may not access, disclose or change data except as authorized by Shelby County Health Department officials, including my supervisor, ISO, and computer staff.

(8) I understand that I may have disciplinary or adverse action, as appropriate, taken against me and may be prosecuted if I use Shelby County Health Department computer systems or resources for any purpose other than performance of Shelby County Health Department business within the scope of my official duties.

(9) I affirm that I have read and understand the provisions and intent of this notice and the importance of preserving computer access security.

(10) Unless and until I am released in writing by an authorized representative of the Shelby County Health Department, I understand that all conditions and obligations imposed upon me by this notice apply during the time I am granted access to the aforementioned computer systems and at all times thereafter."

Computer User's Printed Name:
_____

Computer User's Signature:
_____Date:_____

SHELBY COUNTY HEALTH DEPARTMENT
COMPUTER ACCESS REQUEST FORM

Revised 06-04-12

INFORMATION TO BE FURNISHED BY THE APPLICANT (PLEASE PRINT LEGIBLY)

1) LAST NAME	2) FIRST NAME	3) MIDDLE INITIAL	4) PHONE/EXT

5) POSITION TITLE	6) ROOM #	7) WORK ADDRESS	8) DEPARTMENT:

INFORMATION TO BE FURNISHED BY THE APPLICANT'S SUPERVISOR (PLEASE PRINT LEGIBLY)

9) EMPLOYEE NUMBER	10) SOCIAL (Last 4 Digits)	11) PURPOSE OF REQUEST: ☐ ADD ☐ REMOVE

12) EMPLOYMENT TYPE: (check one) ☐ SCHD Employee ☐ State ☐ Temporary/ Contractor ☐ Volunteer

13) SYSTEM ACCESS REQUEST:

If you are requesting the installation of software not listed under PC Applications, please include your PO number for all software listed under "Other" in the PC Applications section below.

Network Access

- ☐ Active Directory Login
- ☐ Exchange Email
- ☐ AS400
  - ☐ PTBMIS
  - ☐ Library Audit
  - ☐ Other_____

PC Applications

- ☐ Secure Zip
- ☐ Other_____
  - ☐ PO Number_____

Network Applications

- ☐ Client Access (PTBMIS)
- ☐ Breastfeeding Database
- ☐ Coupon Database
- ☐ Departmental Shared Directory
- ☐ HIV Data
- ☐ LABGEMS
- ☐ Logbook
- ☐ NEDDS
- ☐ NETTS
- ☐ REACTOR
- ☐ Ryan White Database
- ☐ Samis
- ☐ STD Client Database
- ☐ TennCare

Network Applications(Cont'd)

- ☐ TIMS
- ☐ TWIS
- ☐ WIC Auto. Grow. Chart
- ☐ OMS
- ☐ Paperless Leave
- ☐ SIGMA
- ☐ Other_____
- ☐ Other_____

Network Printer Access

- ☐ Network Printer One _____
- ☐ Network Printer Two _____

REQUIRED SIGNATURE BY THE REQUESTOR'S SUPERVISOR:

14) Supervisor's Printed Name:	15) Supervisor's Signature:	16) Supervisor's Telephone/Ext:

FORWARD TO SCHD INFORMATION SECURITY OFFICER FOR APPROVAL

17) Security Officer Signature:	18) Date Access Setup/Request Completed:	19) Completed By:

20) Notes:

_____

_____

_____

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
TERMINATING ACCESS TO PHI

Policy # (HS – 202)	**Supersedes Policy**
Approved By	**Effective Date 04-20-05**
HSC _____ Date ____	**Review Date**
CAO _____ Date ____	**Revision Date**

HIPAA Security Language – *Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of the security section.*

SCOPE/APPLICABILITY – This policy applies to all employees, temporaries, interns, volunteers within the Shelby County Health Department, including all personnel affiliated with third parties. This policy applies to all equipment that is owned, leased or maintained by the Shelby County Health Department. The scope of this policy includes all protected health information, as described in the Security Rule.

PURPOSE - The Shelby County Health Department is committed to ensuring the privacy of the department, its employees, and its partners from unauthorized, illegal, and malicious actions by individuals, intentional or unintentional. The Shelby County Health Department's Terminating Access to PHI Policy is intended to ensure the appropriate use of resources and information in the department's existing information systems. Inappropriate use exposes the employee and the Shelby County Health Department to risks including virus attacks, compromise of network systems and services, and legal issues. The purpose of this policy is to outline the standard procedures for termination user accounts within the Shelby County Health Department.

POLICY - It is the policy of the Shelby County Health Department to promptly suspend terminated employees access to electronic protected health information. The Privacy Officer or his/her designate representative is responsible for terminating a user's access to the Shelby County Health Department's Information System.

PROCEDURE

The Shelby County Health Department will terminate access to PHI as follows:

1. The Human Resources Department will ensure that such access to facilities housing EPHI is terminated by:
    (a) retrieving employee's identification badge
    (b) changing card or key access to the facility
    (c) collecting company issued equipment and
    (d) notifying the Information System Administrator or designee of the employee's effective date of separation.
2. The Information System Department will deactivate the separated employee's account to prevent further access to the computer systems using this account.
3. The deactivated account will be purged within 60 days of the employee's termination from the Shelby County Health Department.
4. Prior to the account purge date, the terminating employee's supervisor may request any of the following options, via the Shelby County Health Department's Information System Access Request Form available from information Technologies:
    a. Information maintained at this account be submitted to a forwarding address
    b. Grant another employee access to the terminating employee's e-mail account or review of incoming mail
    c. Enable an out-of-office reply message on the e-mail account to notify mail senders how to redirect their messages
    d. A copy of all files from the deleted user's network directories will be created and presented to the user's Manager for the express purpose of review and assignment of the files as appropriate.
5. If no provisions are made for handling of incoming e-mail, e-mail accounts may be set up to return the mail as undeliverable due to no known recipient.
6. On the account purge date, the following actions will be taken:
    a. E-mail accounts contents will be backed up. Backups will be kept *30* days.
    b. Home directory contents *also* will be backed up for *30 days*.
    c. Accounts will be deleted which will delete e-mail accounts, home directory contents, e-mail account contents and all domain or server accounts.
7. If a restore of backed up data is required, the separated employee's supervisor must make this request to the Shelby County Health Department Information Technologies Help Desk.
8. When possible the Human Resource Personnel will perform exit interviews to address security concerns recommended.

Responsible Parties

Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each health care component. The administrative/management team of each health care component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement

Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment.

Reference
C. F. R. Sec 164.308 (a)(3)(ii)(C)

SHELBY COUNTY GOVERNMENT
SCHD

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
PASSWORD MANAGEMENT

Policy # (HS – 203)	**Supersedes Policy**
Approved By	**Effective Date 04-20-05**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date 04-28-06**

HIPAA Security Language – *Procedure for creating, changing and safeguarding passwords.*

SCOPE/APPLICABILITY – This policy applies to all departments that use, disclose or access protected health information for any purposes. This policy's scope includes all PHI, as described in the Security Rule.

PURPOSE - The SCHD is committed to ensuring that passwords created and used by SCHD workforce to access any network, system, or application used to access, transmit, receive, or store EPHI are properly safeguarded. The purpose of this policy is to establish a standard for the creation and protection of passwords and the frequency of change.

POLICY - Access to SCHD information systems will be supplied to authorized individual users who both submit the appropriate access request paperwork, and supply unique passwords which conform to the rules contained in this policy. This policy applies to all computer and communications systems, regardless of platform or application type, used to access EPHI owned or maintained by the SCHD, its departments, or workforce. All systems require a valid user ID and password. Redundant IDs not assigned to an individual user or administrative function will be deleted or disabled. Additionally, new programs, including third party software and applications developed internally by SCHD must be password protected.

PROCEDURE

General

1. Strong password selection is a mandatory security training requirement. All users must attend security awareness classes conducted by the Security Officer. Training documentation is recorded as outlined in Shelby County Government's HIPAA Privacy and Security Training Policy.
2. All terminals, personal computers, and laptops will be secured with a password protected screen saver, with the automatic activation feature set as defined in the Information Technology Services Network Security Policy (ranging from 15 to 60 minutes) , or by manually locking the workstation when the workstation is unattended.

3. Passwords must be revoked immediately upon resignation, suspension, termination, or work force reduction. It is the duty of the employee's Supervisor to assure that the required Access Form is submitted to SCHD IT.

Password Content

a. All user-chosen passwords must comply with "strong Password construction." The password must be at least eight characters in length, and should consist of a combination of letters, numbers and/or symbols (i.e. # @ $ _).
b. The user should avoid using any combination of their login name or using the same password that they use for personal/ non-work related accounts.
c. Users should not select the following for passwords
   i. names of persons, places or things that easily identify them;
   ii. repeated sequences of letters or numbers;
   iii. a word contained in the English dictionary

4. The SCHD's information system will not grant users selection from the last five previously used passwords.

Password Security

1. Users will not write, display or store passwords in any file, program, command list, procedure, macro or script where the password is susceptible to disclosure or use by anyone other than the owner.
2. Users are required to keep password selection confidential. Sharing of a password or including a password in an e-mail or electronic communication is prohibited.
3. The SCHD will find any workforce member who attempts to use or obtain unauthorized access to another workforce member's password in violation of the SCHD's Confidentiality Policy, and the HIPAA regulation.
4. An employee must promptly report any suspected exposure or unauthorized use of his/her password to the Information Systems Department. The Information System Department will address the password violation the same business day.

Password Expiration

1. Each user must change his/her password every 45 days. After the 45 days expiration period, users will be granted three grace logins before a change is forced. Failure to change the password upon the third notice will result in the password being;
   (a) suspended until reset by a system administrator:
   (b) if dial-up or other external network connections are involved, disconnected.

Password Reset

1. Users requesting a password reset must provide the following information to the SCHD IT Help Desk. Employee Name, Employee Phone Number, Employee

Work Address, Employee ID Number, and the last four digits of the employee's Social Security Number.

2. The user calling in the request must match the user name in the description field of the ID given.
3. All reset passwords will be set to force password change on initial login.
4. All password changes will be documented in a work order. All work orders must include the Employee Name, Employee Phone Number, Employee Work Address, Employee ID Number, and the last four digits of the employee's Social Security Number.
5. Every ID having a password reset will have the new password given only to the employee whose name is in the description field.
6. New passwords may only be given to the Supervisor or Manager of the user assigned the ID with submission of an **Access Request Form** expressly stating that the Manager requires the password to be reset and given to them. The form must be signed, fully executed, and submitted to the SCHD Security Officer prior to the password being changed.

Login Enabling

1. Users requesting their existing user account to be re-enabled must provide the following to the SCHD IT Help Desk; Employee Name, Employee Phone Number, Employee Work Address, Employee ID Number, and the last four digits of the employee's Social Security Number. This does not include resetting of the password, only enabling of a disabled account.
2. All accounts which are re-enabled will be documented in a work order. All work orders must include the Employee Name, Employee Phone Number, Employee Work Address, Employee ID Number, and the last four digits of the employee's Social Security Number.
3. The user calling in the request must match the user name in the description field of the ID given.
4. All re-enabled Id's will have their password options set to force password change on initial login.

Responsible Parties

Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring the HIPAA compliance of each health care component. The administrative/management team of each health care component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement

Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment. Additionally, temporaries and volunteers who do not attend training and fail to furnish document of training will not be allowed to furnish services to SCHD.

Reference
C. F. R. Sec 164.308 (5)(ii)(D)

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
Sanction Policy

Policy # (HS – 204)	**Supersedes Policy**
Approved By	**Effective Date**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date**

HIPAA Privacy and Security Language – *Apply appropriate sanctions against workforce members who fail to comply with the privacy and security policies and procedures of the covered entity.*

SCOPE/APPLICABILITY – This policy applies to all workforce, students, business associates and others who have been granted access to Shelby County Health Department workstations and health information. This policy's scope includes all protected health information, as described in the Privacy and Security Rule.

PURPOSE - The Shelby County Health Department has adopted this policy to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the privacy and security regulations, as well as, to fulfill our duty to protect the confidentiality and integrity of confidential protected health information as required by law, professional ethics, and accreditation requirements.

POLICY - The Shelby County Health Department will ensure compliance with all federal and state privacy and confidentiality laws regarding patient health information. Violations of privacy breaches should be reported to the Privacy Officer and violations of security breaches should be reported to the Security Officer who will in turn work with the Human Resources Officer to resolve the violations in accordance with Shelby County Health Department policies and the appropriate federal and/or state privacy and confidentiality law.

Appropriate sanctions may be based on factors such as the severity, frequency, degree of deviation from expectations, and length of time involved in any privacy violations. However, whether to impose sanctions, and the appropriate sanctions to impose, are always with the discretion of Shelby County Health Department. Shelby County Health Department reserves the right to terminate employment at any time, for any reason, with or without undertaking any of the progressive disciplinary actions outlined in the section entitled "Sanctions for Privacy and Security Violations" on page three of this policy.

REPORTING ALLEGED VIOLATIONS

1. The Shelby County Health Department will train all employees regarding its privacy and security policies and procedures and the manner in which such policies relate to their functions within Shelby County Health Department. See the Shelby County Health Department's HIPAA Policy HS-212 Privacy and Security Training.
2. Members of the Shelby County Health Department workforce are encouraged to report possible privacy and security violations accordingly:
   a. If the violation involves a staff person or patient it should be reported to the immediate Supervisor.
   b. If the violation involves the staff member's supervisor, privacy violations should be reported directly to the Privacy Officer and security violation should be reported directly to Security Officer.
   c. If a privacy or security violation involves a Business Associate it should be reported to the Privacy Officer or Security Officer, respectively. See the section entitled "Disciplinary Steps for Business Associates" on page four of this policy.
   d. When the violation involves the Privacy or Security Officers it should be reported to the Director.
   e. If the violation involves the Director it should be reported to the Chief Administrative Officer of Shelby County Government.
   f. Any other violations should be reported to the United States Department of Health and Human Services
3. If the violation is a privacy breach the Privacy Officer will conduct an investigation. Findings and the appropriate sanctions recommendations will be forwarded to the Human Resources Officer for review. If the violation is a security breach the Security Officer will conduct an investigation and findings and the appropriate sanction recommendations will be forwarded to the Human Resources Officer for review. Also, the Privacy and/or Security Officer will work with the Human Resource Officer to resolve the violation.
4. Investigations must be resolved within five business days. Investigators must document reasons for investigation that last longer than five business days.
5. Confidentiality of all participants in the situation shall be maintained to the extent reasonably possible throughout the investigation. Some circumstances may dictate notification to staff and third parties, but this is at the discretion of the Privacy or Security Officers.
6. Information pertaining to the investigation of breach will only be shared with those who have a need-to-know. This investigation may include, but is not limited to, interviewing the individual accused of the breach, interviewing other individuals, and reviewing pertinent documentation.
7. No Shelby County Health Department officer, employee or agent shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual who files a complaint or reports a possible breach to the integrity or confidentiality of client or other sensitive information, or who cooperates in the investigation or disciplinary procedure arising out of a complaint or report.
8. If the Privacy or Security Officers determine that a privacy or security breach has occurred, the violator will be subject to the appropriate sanctions.

9. A manager or supervisor may also be sanctioned to the extent that inadequate supervision or a lack of due diligence contributed to the violation, or if the manager or supervisor's conduct was punishable or sanction able in other ways. In addition, managers and supervisors may be sanctioned for failing to detect non-compliance with applicable policies and legal requirements, where reasonable diligence would have led to the discovery of any problems or violations.
10. If the investigation of an allegation of a violation concludes that a system, procedure or policy of Shelby County Health Department is responsible for the violation, corrective action will be taken. The Privacy Officer or Security Officer will oversee the implementation of the needed privacy or security change.
11. If an employee is sanctioned, a record of the event and any discipline imposed shall be maintained in the employee's personnel file with a copy to be filed in a master file maintained by the Privacy Officer in accordance with applicable policies of Shelby County Health Department. If deemed necessary, a copy of investigation outcome will be given to the complainant (e.g., when the patient or patient's representative files a complaint).
12. An analysis of reported privacy and/or security breaches shall be prepared by the Privacy and/or Security Officer to be reported the HIPAA Steering Committee, semi-annually.
13. The HIPAA Steering Committee will study the reports to determine privacy and security improvement processes.
14. All information documenting the process noted in this policy regarding the violation will be retained for a period of six years.

SANCTIONS FOR PRIVACY AND SECURITY VIOLATIONS

The following summarizes the types of sanctions that may be imposed by the Shelby County Health Department if a security violation is found to have occurred.

A. Informal Counseling.
B. Verbal Warning.
C. Written Warning.
D. Probation
E. Suspension.
F. Demotion
G. Termination
H. Restitution

DISCIPLINARY STEPS FOR BUSINESS ASSOCIATES

1. Business Associates must adhere to the guidelines for protecting the privacy or security of patient's information as outlined in the business associate agreement between the Shelby County Health Department and the Business Associate.
2. An employee, agent, contractors or other should notify the Shelby County Health Department Privacy Officer should he/she become aware of a privacy violation. An employee, agent, contractors or other should notify the Shelby County Health Department Security Officer should he/she become aware of a security violation.

3. The Privacy Officer or Security Officer will investigate the complaint to determine if the reported violation is factual and the appropriate action. Violation by the contracted vendor may result in corrective action up to and including termination of the agreement.
4. All investigation should be resolved within ten business days. The Privacy Officer or Security Officer must document the reason an investigation lasted longer than ten business days.
5. An analysis of reported privacy and/or security breaches shall be prepared by the Privacy and/or Security Officer to be reported the HIPAA Steering Committee, semi-annually.
6. The HIPAA Steering Committee will study the reports to determine privacy and security improvement processes.
7. All information documenting the process noted in this policy regarding the violation will be retained for a period of six years.

Responsible Parties

Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each health care component. The administrative/management team of each health care component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement

Employees, including students violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment. Violation of this policy by the business associate may result in corrective action up to and including termination of the agreement. In some cases, civil and criminal penalties for misuse or misappropriation of health information and electronic media may occur. The violator should expect that the Shelby County Health Department shall provide information concerning the violation to appropriate law enforcement personnel and will cooperate with any law enforcement investigation or prosecution.

Reference

45 C.F.R. Sec. 164.310 (b)

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
Security Incident Response and Reporting

Policy # (HS – 205)	**Supersedes Policy**
Approved By	**Effective Date**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date**

HIPAA Security Language – *Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.*

SCOPE/APPLICABILITY – All individuals granted access to the Shelby County Health Department information system are required to comply with the procedures contained in this Policy. This includes full, part-time and temporary employees, volunteers, contractors, persons employed by contractors who perform work on behalf of the Shelby County Health Department, and others authorized to access the Shelby County Health Department information, network and/or systems.

PURPOSE: The HIPAA Security Rule requires the Shelby County Health Department to establish an incident response and reporting process to address the handling of privacy and information security incidents. The purpose of this policy is to provide quick, effective and efficient response to privacy and information security incidents ranging from unauthorized intrusions into the Shelby County Health Department network systems to the mishandling of data that may compromise the confidentiality, integrity or availability of the Shelby County Health Department EPHI.

POLICY
All suspected or known incidents that threaten the security of the Shelby County Health Department's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Shelby County Health Department's information technology systems shall be reported to the Security Officer. Such reports shall be submitted within 24 hours of the discovered occurrence.

Procedure
1. Section Managers/Supervisors must assure that all employees, students, or volunteers who are assigned under their supervision as a new hire, promotion,

demotion, transfer, or temporary assignment receive the appropriate level of HIPAA security training. This training material will be provided by the Security Officer in the form of a presentation and copies of the HIPAA security policies during the annual HIPAA Train-The-Trainer sessions and will contain information on handling security incidents, reporting procedures, and how to avoid risks.

2. All Business Associates and Memorandum of Understanding Agreements shall contain HIPAA complaint requirements that contractors must follow to report security incidents.
3. All employees should report any privacy or information security incident to the department manager/supervisor, immediately.
4. If the manager/supervisor is unavailable or believed to be the suspected violator, the employee shall report the incident directly to the Security Officer.
5. The reporting of security incidents should be documented on the Shelby County Health Department's *Security Incident Reporting Form*. A sample *Security Incident Reporting Form* is attached. See the Security Officer for hard copies. The form should be completed in its entirety including full details regarding the incident.
6. The security incident should be reported to the Security Officer by one of the following methods:
   (A) E-mail or
   (B) Interdepartmental/Hand mail
   1. **E-MAIL** - Employees reporting via e-mail may obtain access to the *Security Incident Reporting Form* to document the suspected activity from the Security Officer by emailing and requesting a copy of the form. The completed form should be e-mailed to the Security Officer. The address is smcclure@co.shelby.tn.us
   2. **INTERDEPARTMENTAL/HAND** - Employees reporting via interdepartmental mail or hand delivery, may obtain access to the *Security Incident Reporting Form* to document the suspected activity by copying their copy attached to this policy, or by seeing the Security Officer for a hard copy, or contacting the Security Officer requesting either email or hard copies. The completed form should be inserted into an interdepartmental envelope. The interdepartmental envelope should indicate the Security Officer's name and the Information Technology Department as the address to deliver the reported information.
7. Upon receipt of the *Security Incident Reporting Form*, the Security Officer shall:
   Document the date of receipt upon the form;
   (A) Investigate, mitigate and/or recommend department heads resolve any harmful effect of the incident known to the extent practicable. Additionally, the Security Officer shall ensure that the Director, Privacy Officer, Human Resources and other appropriate Administrative personnel are informed of the mitigation and/or participate in the mitigation process. The level of participation will be determined by the severity of the security incident and its relationship to the personnel's organizational responsibilities;

(B) In the event of a security-related breach, the Security Officer will complete the requirements of the "Notification of Breach of 'Unsecured' Protected Health Information (PHI)" Policy HS-214.
(C) Facilitate privacy and information security related process improvement activities to reduce the risk of repeated incidents;
(D) Maintain, to the extent reasonably, possible the confidentiality of all participants involved;
(E) Resolved, completed and closed incident reports will be maintained within the Privacy Office.

Responsible Parties
Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each Health Care Component. The administrative/management team of each Health Care Component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement
Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment. Additionally, termination of services or contracts will be part-time employees, volunteers, contractors, temporary workers, those employed by others to perform work on behalf of the Shelby County Health Department, and others authorized to access Shelby County Health Department information, network, and/or systems.

Reference
C. F. R. Sec 164.308 (a)(7)(ii)(E)

	SHELBY COUNTY GOVERNMENT **Security Incident Reporting Form**	**Security Office Use Only** **Date Received _____** **Received By _____**

Instructions: ***This form shall be used to report any acts or omissions that result in (1) the attempted or successful unauthorized access, use, disclosure, modification or destruction of information; or (2) interference with system operations in an information system. If additional information is required, you will be contacted via phone or e-mail. To assist with our initial assessment and investigation, please provide as much information as possible.***

REPORTING INFORMATION

I. Employee (s) Involved _____
Incident Discovery Date ____________
Title (s) _____
Department _____

II. Business Association's Name _____
Incident Discovery Date ____________

III. Description of the Incident (include PHI released)

_____

_____

_____

_____

_____ ____________ _____

Signature **Date** **Telephone Number**

SECURITY OFFICE USE ONLY

IV. System Compromised/Damaged Caused _____

_____

_____

_____

_____

_____

V. Investigation Details _____

_____

_____

_____

_____

_____

_____

_____

VI. Remedy Implemented _____

VII. Sanctions _____

_____ ____________

Signature of Security Officer **Date**

Shelby County Health Department

HIPAA Security Incident Report Log

Date Received	Site	Nature Of Complaint	Breach Status	Disposition	Completion Date

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
Applications and Data Criticality Analysis

Policy # (HS – 206)	**Supersedes Policy**
Approved By	**Effective Date**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date**

HIPAA Security Language – *Assess the relative criticality of specific applications and data in support of other contingency plan components.*

SCOPE/APPLICABILITY – This policy applies to all departments that use, disclose or access protected health information for any purposes. This policy's scope includes all protected health information, as described in the Security Rule.

PURPOSE: The Shelby County Health Department must develop a plan to ensure critical business processes for the protection of electronic health information continues while the Shelby County Health Department is operating in emergency mode. This policy formally documents the steps to be taken by the Shelby County Health Department to protect patient's electronic health information in an emergency situation.

POLICY
The Shelby County Health Department will establish, and implement as necessary, procedures to enable continuation of processes for the protection and security of electronic protected health information while operating in the emergency mode. The Shelby County Health Department will use the Emergency Operation Mode Plan only during and immediately after a crisis situation.

Procedure
1. If it is decided that this addressable specification is already addressed by another safeguard, the Security Officer will document this fact and present this documentation to management for approval. The Security Officer is responsible for the development and implementation of this specification, as described below, in as much as it is not previously covered by another safeguard, such fact having been documented and presented to management.

2. To adequately support business operations during a disaster or emergency, the Shelby County Health Department will perform an assessment of the vulnerabilities and

security of the applications and information systems that process or store EPHI. This will be done as part of the Risk Analysis. (See Risk Analysis).

3. The Security Officer will assess and analyze the criticality of these applications and information systems for the development and updating of the Shelby County Health Department Data Backup, Disaster Recovery, and Emergency Mode Operation Plans. See Data Backup and Disaster Recovery Plan and Emergency Mode Operation Plan.

4. The risk assessment and analysis will include the following:

   - Identification of risks and potential resource dependencies.
   - Identification of critical business processes with associated applications and EPHI.
   - Identification of single points of failure for continuing critical business operations.
   - Ranking of the critical applications and EPHI in order of priority.
   - Determination of appropriate recovery solutions (e.g., hot site, cold site).

5. The application and Risk Analysis will be conducted at least every two years or when significant changes occur to applications or information systems that process or store EPHI, or significant revisions are made to the Shelby County Health Department's Data Backup and Disaster Recovery Plan or Emergency Mode Operation Plan.

6. Documentation generated from the Risk Analysis will be maintained for ten years from the date of creation or from the date it was last in effect.

Responsible Parties
Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each Health Care Component. The administrative/management team of each Health Care Component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement
Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment. Additionally, temporaries and volunteers who do not attend training and fail to furnish document of training will not be allowed to furnish services to the Shelby County Health Department.

Reference
C. F. R. Sec 164.308 (a)(7)(ii)(E)

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
Emergency Mode Operation Plan

Policy # (HS – 207)	**Supersedes Policy**
Approved By	**Effective Date**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date**

HIPAA Security Language – *Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.*

SCOPE/APPLICABILITY – This policy applies to all departments that use, disclose or access protected health information for any purposes. This policy's scope includes all protected health information, as described in the Security Rule.

PURPOSE: The Shelby County Health Department must develop a plan to ensure that critical business processes protect electronic health information while the Shelby County Health Department operating in emergency mode. This policy formally documents the steps to be taken by the Shelby County Health Department to protect patient's electronic health information in an emergency situation.

POLICY
The Shelby County Health Department will establish, and implement as necessary, procedures to enable the continuation of critical business processes protecting the security of electronic protected health information while operating in the emergency mode. The Shelby County Health Department will use the Emergency Operation Mode Plan only during and immediately after a crisis situation.

Procedure
1. The Security Officer holds the chief responsibility for the maintenance of the departmental Emergency Operation Mode Plans including annual Security Committee review of plans with their respective departments. These plans will contain procedures to enable critical business process to continue operating while the Shelby County Health Department is functioning in emergency mode.
2. Department Managers are responsible for developing Emergency Mode Operation plans for their departments, including manual procedures that will enable continuation of critical business processes until the system has been restored, and submitting these to the Security Officer.

3. The Emergency Mode Operation Plan will be an integral part of the Shelby County Health Department's overall contingency plan, which contains processes enabling the Shelby County Health Department to continue to operate in the event of emergencies or disasters such as fire, vandalism, terrorism, natural disaster, or system failure. See the Shelby County Health Department Disaster Recovery Plan Policy and Applications and Data Criticality Analysis Policy.
4. The results of the Risk Analysis and Applications and Data Criticality Analysis will help determine the elements to be included in the Shelby County Health Department Emergency Mode Operation Plan. Emergency Mode Operation Plans will include the following elements.
    - Identification of critical systems, applications, processes, and EPHI.
    - List of workforce member or team and associated roles.
    - Ranking of applications, processes and EPHI according to priority for critical business processes continuation.
    - Determination of permissible unavailability of systems(i.e., disruption of service, use, or access for applications, processes and EPHI).
    - Identification of Emergency Mode Operation Plan activation triggers (for example, system disruption for greater than one hour, natural disaster resulting in physical damage to systems, etc.).
    - Process for securing human resources if workforce members are physically or geographically unavailable.
    - Chain of command that has responsibility for activating the Emergency Mode Operation Plan.
    - Plan for communicating the activation and status of the Emergency Mode Operation Plan to others.
    - Identification of the backed up critical applications, data, operating software, and databases as defined in the Data Backup Plan and its associated Policy.
    - Identification of recovery process for systems, applications and EPHI.
    - Identification of alternate business operations processing sites within or outside the organization.
    - Alternate site operating procedures.

5. Workforce members will be trained regarding the specific policies and procedures to be followed when the Emergency Mode Operation Plan is activated.
6. The current Emergency Mode Operation Plan documentation will be maintained indefinitely or until the Emergency Mode Operation Plan is no longer required. In addition, the prior Emergency Mode Operation Plan will be maintained indefinitely or until the current EMOP is revised. Two versions of the plan will always be maintained.
7. Each department will be responsible for the testing of their respective EMOPs.
8. The appropriated workforce members will receive training on the authorization process.
9. Any workforce member found to have violated this policy will be subject to a appropriate disciplinary action as defined in the Shelby County Health Department HIPAA Privacy and Security Sanction Policy.

Responsible Parties
Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each Health Care Component. The administrative/management team of each Health Care Component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement
Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment. Additionally, temporaries and volunteers who do not attend training and fail to furnish document of training will not be allowed to furnish services to the Shelby County Health Department.

Reference
C. F. R. Sec 164.308 (a)(7)(ii)(C)

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
Security Testing & Revision Policy

Policy # (HS – 208)	**Supersedes Policy**
Approved By	**Effective Date**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date**

HIPAA Security Language – *Implementation procedures for periodic testing and revision of contingency plans.*

SCOPE/APPLICABILITY – The procedure applies to all Shelby County Health Department employees, agents and contractors involved in the contingency planning process. The procedure defines testing and revision steps to be contained in all the Shelby County Health Department Business Continuity Plans.

PURPOSE: To ensure the smooth implementation of procedures for responding to emergencies and to assure continued support for critical functions.

POLICY
The Shelby County Health Department will test all elements of the contingency plan to determine that the various components will provide necessary functionality and protect the security of patient information. Each component of the contingency plan will be tested individually. Once the individual components have been tested, staff members with specific responsibilities in the recovery operation must be given an opportunity to practice their roles in a realistic test situation. A final test of the contingency plan will be conducted to simulate the response to a complete systems failure. The results of the final test should be evaluated by the Executive Director and Security Officer. The contingency plan should be revised as appropriate, in response to the test.

PROCEDURES
1. The HIPAA Security Awareness Training Program will include a training module relative to how personnel shall react in the event of a disaster or other business interruption. The training will be presented to the Shelby County Health Department's staff annually.
2. Department managers are responsible for periodic testing of their emergency mode operations plan.

3. The results of these tests will be logged in a centralized location determined by the HIPAA Security Officer and will include documentation on revisions made to the data backup and/or disaster recovery plans.
4. The HIPAA Security Officer will document disaster recovery test results and share the results with the participants.
5. The HIPAA Security Officer will require departmental backup and restore of data as a part of the periodic disaster recovery testing.
6. The HIPAA Security Officer will test the procedure anytime new software programs are installed on the Shelby County Health Department computers to ensure data can be backed up, restored and operational within the timeframe established by the Shelby County Health Department Disaster Recovery Policy.
7. All users must be familiar with the contingency plan procedures and must thoroughly be briefed on pertinent aspects of the plan.
8. The Shelby County Health Department will conduct testing and revision, every two years.

Responsible Parties
Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each health care component. The administrative/management team of each health care component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement
Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment.

Reference
45 C.F.R. Sec. 164.308 (a) (7)

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
Periodic Evaluation

Policy # (HS – 209)	**Supersedes Policy**
Approved By	**Effective Date**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date**

HIPAA Security Language – *Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirement of the security regulation.*

SCOPE/APPLICABILITY – To ensure that each HIPAA Security Policy and Procedure developed and implemented by the Shelby County Health Department is periodically evaluated for technical and non-technical viability.

PURPOSE - The Shelby County Health Department is committed to conducting business in compliance with all applicable laws, regulations and the Shelby County Health Department's policies. The Shelby County Health Department has adopted this policy to establish periodic guidelines for reviewing the effectiveness of the Shelby County Health Department's Security Policies and Procedures.

POLICY -

Initial Evaluation

Prior to the HIPAA Security compliance date, the Shelby County Health Department Security Officer should evaluate its existing Security Policies and Procedures to determine their compliance with the Security Regulations. Once compliance with the Security Regulations is established, the Security Polices and Procedures of the Shelby County Health Department shall be evaluated on a periodic basis to assure continued viability in light of technological, environment or operational changes that could affect the security of EPHI.

Technical and Non-Technical Evaluations

The Shelby County Health Department's Security Officer must periodically (at least annually) evaluate its HIPAA Security Procedures to ensure that such procedures maintain their technical and non-technical viability and continue to comply with the HIPAA Security Policies. The Shelby County Health Department's Security Officer will

conduct this evaluation prior to annual evaluations conducted by Shelby County Government.

Non-Technical Evaluation

(a) The Health Policy Coordinator will review on an annual basis the viability of the Shelby County Health Department's Security Policies and Procedures.

(b) The Health Policy Coordinator will develop and recommend to the HIPAA Security Subcommittee any necessary Security Policy.

Technical Evaluation

Shelby County Government's (SCG) Information Technology Security Analyst will perform technical evaluations accordingly:

1. The Information Technology Security Analyst will develop and ensure the implementation of a standard procedure for performing HIPAA compliant evaluations.
2. The Security Analyst shall conduct an evaluation of the Shelby County Health Department's compliance to technical HIPAA security standards on a scheduled basis.
3. Technical evaluations shall be conducted when there is an environmental or operational change that possibly affects the confidentiality, integrity, or availability of electronic protected health information.
4. Results of non-compliance shall be remediated as soon as practicable, depending on specific circumstances and the acceptability of the risk determined by the Shelby County Health Department's Security Officer and Director.
5. Results of all technical evaluations shall be securely stored using authorized mechanisms identified by the (SCG) Information Technology Security Analyst.

Periodic Evaluation

(a) The HIPAA Policy Development Subcommittee will reconvene on an annual basis to evaluate the technical and non-technical viability of the Shelby County Health Department's Security Policies. It is the responsibility of the Shelby County Government Health Policy Coordinator to reconvene the HIPAA Subcommittee in accordance with this Policy.

(b) Any member of the HIPAA Steering Committee, the HIPAA Technical Subcommittee, HIPAA Policy Development Subcommittee, or Shelby County employee may suggest changes to the Security Policies and Procedures by submitting such suggestions to the HIPAA Policy Development Subcommittee for consideration.

(c) The HIPAA Policy Development Subcommittee will review suggested Security Policy or Security Procedure changes and make a preliminary recommendation.

(d) If the HIPAA Policy Subcommittee preliminarily recommends a new security standard or a change in the Shelby County Health Department's Security Policies or Procedures, such changes will be communicated to the Shelby County Health Department by the Shelby County Health Department's Security Officer, who

will elicit feedback for a specific period of time and provide such feedback to the HIPAA Policy Subcommittee.

(e) The HIPAA Policy Subcommittee will consider the feedback received and make a final recommendation on the suggested change to the HIPAA Steering Committee.

(f) If the HIPAA Steering Committee approves the change, such change will be communicated to all Shelby County Health Department employees through timely incorporation into existing or new policies and issuance of said policies to all Shelby County Health Department employees.

Evaluation Upon Occurrence of Certain Events

(a) In the event that one or more of the following events occur, the policy evaluation process described in section five under policy will be immediately triggered upon:

- Changes in the HIPAA Security or Privacy Regulations
- New federal, state, or local laws or regulations affecting the privacy or security of PHI
- Changes in technology, environmental processes or business processes that may affect HIPAA Security Policies or Security Procedures, or
- A serious security violation, breach, or other security incidents occurs

(b) The Health Policy Coordinator may reconvene the HIPAA Policy Development Subcommittee, if deemed necessary, based on information received from the HIPAA Privacy Officer, the HIPAA Compliance Office, Internal Audit, a HIPAA Technical Security Subcommittee Member, of the HIPAA Steering Committee, or other relevant sources.

Responsible Parties

Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each Health Care Component. The administrative/management team of each Health Care Component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement

Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment. Additionally, temporaries and volunteers who do not attend training and fail to furnish document of training will not be allowed to furnish services to the Shelby County Health Department.

Reference

C. F. R. Sec 164.308 (a)(8)

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
WORKFORCE CLEARANCE POLICY

Policy # (HS –210)	**Supersedes Policy**
Approved By	**Effective Date 04-20-05**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date 02-05-07**

HIPAA Security Language – *Implement procedures to determine that the access of a workforce member to EPHI is appropriate.*

SCOPE/APPLICABILITY – This policy applies to all departments that use or disclose protected health information for any purposes. This policy's scope includes all protected health information, described in the Security Rule.

PURPOSE: This policy represents the Shelby County Health Department's commitment to ensure that all workforce members have appropriate authorization to access Shelby County Health Department information systems containing EPHI.

POLICY: The background of all Shelby County Health Department workforce members must be adequately reviewed during the hiring process. When defining an organizational position, the Shelby County Health Department's human resources department and the hiring manager must identify and define both the security responsibilities of and level of supervision required for the position. All Shelby County Health Department workforce members who access the Shelby County Health Department's information systems containing EPHI must sign a confidentiality agreement.

PROCEDURE

1. The background of all the Shelby County Health Department's workforce members must be adequately reviewed during the hiring process. Any employees accessing EPHI will be subject to the following verification checks:
   - Character references
   - Confirmation of claimed academic and professional qualifications
   - Professional license validation

3. When defining a position, the Shelby County Health Department human resources department and the hiring manager must identify the security responsibilities and supervision required for the position. Security responsibilities include general

responsibilities for maintaining security, as well as any specific responsibilities for the protection of the confidentiality, integrity, or availability of Shelby County Health Department information systems or processes.

4. When job candidates are provided via an agency, the Shelby County Health Department's contract with the agency must clearly state the agency's responsibilities for reviewing the candidates' backgrounds according to requirements listed in section one of the procedures for this policy.

5. It is the responsibility of each Shelby County Health Department sections that retain the services of a third party to ensure that the party or person(s) adheres to all appropriate Shelby County Health Department policies.

6. All Shelby County Health Department workforce members who access the Shelby County Health Department's information system containing EPHI must sign a confidentiality agreement in which they agree not to provide EPHI or to discuss confidential information to which they have access to unauthorized persons.

Responsible Parties
Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring the compliance of each health care component. The administrative/management team of each health care component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement
Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment.

Reference
45 CFR 164.308 (a)(3)(ii)(B)

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
INFORMATION SYSTEM BACKUP PLAN

Policy # (HS – 211)	**Supersedes Policy**
Approved By	**Effective Date**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date**

HIPAA Security Language – *Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.*

SCOPE/APPLICABILITY – This policy applies to all critical data files and operations of the Shelby County Health Department that contain protected health information as defined by the HIPAA Privacy and Security Rule.

PURPOSE: All electronic information considered of institutional value should be copied onto secure storage media on a regular basis for disaster recovery and business resumption. This policy outlines the minimum requirements for the creation and retention of backups. Special backup need*s* identified through technical risk analysis, which exceed these requirements, should be accommodated on an individual basis.

POLICY - The Shelby County Health Department must implement an adequate backup plan to ensure the recovery of data and systems in the event of failure. The backup provision will allow the Shelby County Health Department's business processes to be resumed in a reasonable amount of time with minimal loss of data. Since hardware and software failures can take many forms, and may occur over time, multiple generations of institutional data backups should be maintained.

PROCEDURES

1. The Shelby County Health Department's Security Officer is responsible for establishing, maintaining and executing written procedures for backup and restoration of production systems.

2. Backups of all institutional data must be retained such that all systems are fully recoverable. This may be achieved using a combination of image copies, incremental backups, differential backups, transaction logs, or other techniques.
3. The frequency of backups is determined by the volatility of data; the retention of backup copies is determined by criticality of the data. At a minimum, backups

must be retained for 20 days in the case of daily backups, 10 months in the case of monthly backups, and 9 years in the case of yearly backups.

4. At least three versions of the data must be maintained.
5. At a minimum, one fully recoverable version of all critical data must be stored in a secure, off-site location. The data must be labeled, packed, and transported to the off-site storage facility securely.
6. Each container entering or leaving the 814 Jefferson location must have a "Offsite Container Sign-in / Sign-out Form" fully completed. This form is to be filed in the "Offsite Container Records" folder located in the Information Technologies file cabinet, and is to be maintained indefinitely.
7. The storage facility must have controlled access, proper environmental controls and true floor to ceiling walls.
8. Access control to facility information stored off-site should be stringently controlled. Locks and/or personnel will be used to control the off-site storage to prevent unauthorized access.
9. System and application documentation and an up-to date copy of the contingency plans will also be stored securely at the off-site location.
10. Derived data should be backed up only if restoration is more efficient than creation in the event of failure.
11. All critical information used on workstations should be placed on networked file server drives to allow for backup.
12. Backup documentation includes identification of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period.
13. Documentation of the restoration process must include procedures for the recovery from single-system or application failures as well as for a total data center disaster scenario.
14. Backup and recovery documentation will be reviewed and updated regularly to account for new technology, business, and migration of applications to alternative platforms.
15. Recovery procedures will be tested on an annual basis.

Responsible Parties

Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each health care component. The administrative/management team of each health care component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement

Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment.

Reference

45 C.F.R. Sec. 164.308 (a)(7)

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
Risk Management Policy

Policy # (HS – 212)	**Supersedes Policy**
Approved By	**Effective Date**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date**

HIPAA Security Language – *Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriated level.*

SCOPE/APPLICABILITY – The scope of this Policy covers the periodical ePHI risk analyses that the Shelby County Health Department will conduct and the security measures and safeguards that the Shelby County Health Department will implement based upon such risk analyses.

PURPOSE - The Shelby County Health Department is committed to conducting business in compliance with all applicable laws, regulations and the Shelby County Health Department's policies. The Shelby County Health Department has adopted this policy to ensure that security violations are prevented, detected, contained and corrected in accordance with the HIPAA Security Regulation.

POLICY - The Shelby County Health Department will take effective steps to minimize or eliminate any potential risk and vulnerabilities to the electronic protected health information stored or transmitted by the Shelby County Health Department's information system. The Shelby County Health Department shall continually assess potential risks and vulnerabilities to protected ePHI in its possession, and develop, implement, and maintain appropriate security. The Shelby County Health Department will implement a comprehensive risk management process that includes:

- Processes to track industry-posted vulnerabilities, either devising corrective actions in order to remediate the risks, or making conscious decisions to accept the risks posed by the vulnerabilities.
- Processes to perform security assessments periodically as vulnerabilities are continuously being identified within the industry.
- Documentation of the threats and vulnerabilities to the systems and network.
- Presentation of the issues identified during the security assessments to management.
- Identification of options and associated cost for remediation.

- Processes to make necessary changes to the continuity plan based on the results of the risk assessment.
- Documentation of security implementation decisions including the information used to make those decisions (usually based on the risk analysis) and the supporting rationale.

PROCEDURE

1. Prior to the HIPAA Security Rule compliance date, the Shelby County Health Department's Security Officer will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the Shelby County Health Department.
2. The Risk Assessment will be performed in accordance with the National Institute of Standards Technology (NIST) Guidelines recommended by the HIPAA Security Rule. The risk assessment methodology will encompass the nine primary NIST steps listed below:
   (a) Determine system characterization by reviewing hardware; software; system interfaces; data and information; and people.
   (b) System mission.
   (c) Identify any vulnerability or weaknesses in security procedures or safe guards.
   (d) Identify events that can negatively impact security (natural or human factors).
   (e) Identify current controls in place.
   (f) Identify the potential impact that a security breach could have on an organization's operations or assets, including loss of integrity, availability, or confidentiality.
   (g) Recommend security controls for the information and the system, including all the technical and non-technical protections in place to address security concerns.
   (h) Determine residual risk.
   (i) Document all outputs and outcomes from the risk assessment activities. Consolidate all lists of outputs and outcomes into a single list of documented risks for best practices purposes.
3. The risk analysis shall demonstrate, at a minimum, the following information:
   a. The level of risk associated with each potential vulnerability exploitation,
   b. Steps to be taken to reduce the risk of vulnerability exploitation, and
   c. Processes for maintaining no more than the acceptable level of risk.
4. HIPAA Technical Security Subcommittee will review the risk assessment reports, make recommendations to reduce non-compliant and unacceptable risks to a reasonable and appropriate level.
5. The mitigation decisions, additional procedures (if applicable) and responsibilities assigned will be documented and maintained by the Shelby County Health Department's Security Officer.
6. Unresolved risks and/or risks associated with a cost will be presented to Senior Administration for review and action. Senior Administration may accept the risks, provide necessary resources to mitigate the risk, or temporarily accept the risk and define future plans for risk mitigation.

7. The decisions by Senior Administration will be maintained on file in the (Health Care Component's) Information Security and Shelby County Health Policy Coordinator offices.
8. Results of all risk analysis shall be securely stored using authorized mechanism determined by the Security Officer. The ePHI will be identified and logged into a common catalogue (www.ephi. MSHD.com). An ePHI repository may be in the form of a database, spreadsheet, folder, storage device, document or other form of electronic information that is accessed by one or more users. Each repository will be logged with the appropriate level of file, system, and owner information including, but not limited to:

- Repository Name
- Responsibility Party's name
- Contact Information
- Number of Users that access the repository
- Number of Records
- System Name
- System IP Address (where applicable)
- System Location
- System Manager
- System Manger Contact Information
- Risk Level

Each division must update its ePHI inventory at least annually to ensure that the ePHI catalogue is up to date and accurate.

9. The Shelby County Health Department's Security Officer will conduct a risk assessment every two years, after a significant audit finding or when the information system experiences significant enhancement or modification. The assessment will be conducted by April 20th of each year beginning in 2007.

Responsible Parties
Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each health care component. The administrative/management team of each health care component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement
Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment.

Reference
45 C.F.R. Sec. 164.308 (a)(1)

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
PRIVACY AND SECURITY TRAINING

Policy # (HS – 213)	**Supersedes Policy**
Approved By	**Effective Date**
HSC _____ Date ____	**Review Date**
CAO _____ Date ____	**Revision Date**

HIPAA Privacy and Security Language – *A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by the Privacy Rule, as necessary and appropriate for the members of the workforce to carry out their job responsibilities. The covered entity must also implement a security awareness and training program for all members of its workforce (including management).*

SCOPE/APPLICABILITY – This policy applies to all departments that use, disclose or access protected health information for any purposes. This policy's scope includes all protected health information, as described in the Privacy and Security Rule.

PURPOSE: The Shelby County Health Department has always regarded patient health information as strictly confidential. The Health Insurance Portability and Accountability Act (HIPAA) is another opportunity for the Shelby County Health Department to improve its confidentiality and privacy practices. Accordingly, The Shelby County Health Department has developed an ongoing employee privacy and security awareness training program designed to enhance the confidentiality culture within its institution.

POLICY
The Shelby County Health Department will train all employees regarding its privacy and security policies and procedures and the manner in which such policies relate to their function within the Shelby County Health Department. In accordance with the Security Rule, the Shelby County Health Department's will include topics specific to the following areas in the security awareness and training program:

- Security reminders
- Protection from malicious software
- Log-in monitoring and
- Password management

Each employee will be required to attend in-service training programs that focus on federal and state laws relative to the privacy of patients' health information.

PROCEDURE

1. The Shelby County Health Department's Privacy and Security Officers will develop HIPAA Privacy and Security training material, respectively.
2. All training materials will include a quiz or some other mechanism to demonstrate understanding of the information presented.
3. Prior to training employees, the Privacy and Security Officers must submit training material to the Health Policy Coordinator for review.
4. The trainers will include the Shelby County Health Department's Privacy Officer, Security Officer, and the Department Manager or Designee.
5. Training will be offered to full-time, part-time, and temporary employees, students, interns, and volunteers.
6. Privacy awareness training will be furnished to each workforce member on or before April 14, 2003. Security awareness training will be furnished to each workforce member on or before April 21, 2005.
7. The Shelby County Health Department's management team will be accountable for providing the opportunity and direction to the employee to achieve the training and education required by this policy. Management must ensure that each employee within his/her department:
    a. attends and completes the required initial and refresher privacy and security training sessions,
    b. receives departmental specific privacy and security policy and procedure training, and
    c. complies with institutional and departmental specific training and requirements.
8. Training for new employees will be incorporated into new employee orientation. Orientation will be conducted within thirty (30) days of employment.
9. When a member of the health care component's workforce transfers from one department to another, the workforce member shall be trained on the new departmental specific policies and procedures within thirty (30) days of being assigned to the new department.
10. Additional training will be provided to workforce whose functions are affected by a material change in the policies and procedures required by the privacy and security regulation, or environmental and operational changes communicated to the Security Officer. Training will be conducted within thirty (30) days of the change.
11. Annual employee refresher training will be conducted by the Shelby County Health Department's management team. Employee refresher training must be completed by April 14th of each year.
12. During the initial training, each employee will be required to sign the attendance record, training record and a confidentiality statement. Employees are required to re-sign the attendance and training records each training session and re-sign the confidentiality statement when changes are made to the statement.
13. Privacy and Security training will be documented accordingly:
    a. the Privacy Officers will maintain record of training presentation, attendance and training records and confidentiality statements,
    b. a signed confidentiality statement will be filed in each employee's record;
    c. a privacy and security training record will kept in each employee's file,

d. the Privacy Officer will submit a copy of training documentation to the Health Policy Coordinator; and
e. documentation regarding training will be maintained in written or electronic format, for at least (6) years.

14. The Health Policy Coordinator will assume the following training responsibilities:
    a) conduct semi-annual HIPAA workshops for each covered entity,
    b) disseminate material changes to the Privacy and Security rule within ten (10) business days of change,
    c) review and assist with training presentations, and
    d) maintain documentation of training as mentioned in section twelve (12) of this policy.
15. The Shelby County Health Department will retain documents enumerated in the above section for six (6) years from the date it was created, the date it was received or the date it was last in effect, which ever is later.

Responsible Parties

Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each health care component. The administrative/management team of the Shelby County Health Department must ensure that sections under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliance duties.

Enforcement

Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment. Additionally, temporaries and volunteers who do not attend training and fail to furnish document of training will not be allowed to furnish services to the Shelby County Health Department.

Reference

C. F. R. Sec 164.530 (b)
C. F. R. Sec 164.308 (a) (5) (i)

SHELBY COUNTY GOVERNMENT
(HEALTH CARE COMPONENT)

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY
Notification of Breach of "Unsecured" Protected Health Information (PHI)

Policy # HS-214	**Supersedes Policy**
Approved By	**Effective Date**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date**

SCOPE: *This policy applies to all workforce members of (insert name) and Shelby County Government (SCG) divisions that receive, maintain or transport protected health information on behalf of the Shelby County Government designated HIPAA health care components. This policy's scope includes all protected health information, as described in the HIPAA Privacy and Security Rules and HITECH regulation.*

PURPOSE: Shelby County Government is a hybrid HIPAA covered entity that is required by law to protect the privacy of individuals' health information. SCG must notify individuals and certain entities regarding a breach of protected health information not secured according to the National Institute Standards for Technology adopted by HITECH regulation. In accordance with regulatory requirements, if a breach of "unsecured" protected health information occurs SCG must notify the individual and certain entities. The purpose of this policy is to establish a procedure for notifying the appropriate individuals and entities if such breach should occur

DEFINITION: Breach: For the purposes of the policy, the term "breach" means the acquisition, access, use or disclosure of protected health information in a manner not otherwise permitted under the HIPAA Privacy and Security Rule which compromises the security or privacy of the protected health information. The term "protected health information" means any information, including very basic information such as their name or address, that (1) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (2) either identifies the individual or could reasonably be used to identify the individual.

POLICY: It is the responsibility of SCG to protect and preserve the confidentiality of all protected information held by the County or other entities on its behalf. In an effort to minimize breach related risks, SCG has implemented administrative, physical and technical safeguards to protect the health information entrusted to the County. Employees will be trained regarding their responsibility for reporting suspected breaches. In an effort to minimize financial, reputation or other harm to the affected individuals,

employees are required to report the privacy breaches to the Privacy Officer and to report security/system related breaches to the Security Officer. The Privacy and Security Officer will be responsible for investigating suspected breaches in their respective HIPAA task related area. Upon completion of the investigation, the Privacy or Security Officer will notify the individual (s) and appropriate entities of cases determined to be breaches.

Procedure

1. Any member of SCG's Health Care Components or divisions and departments that handles protected health information on behalf of the Health Care Component who knows, believes, or suspects that a breach of protected health information has occurred must report the breach immediately to the Privacy or Security Officer.
2. The employee discovering the breach must follow any available precautions to contain the breached information from further harm while waiting on the Privacy or Security Officer immediate response.
3. The Privacy Officer and Security Officer will investigate and resolve privacy breaches and computer security breaches, respectively.
4. After a potential breach is reported, the Privacy and/or Security Officer will work with other officials and departments, including the Compliance Officer and HIPAA Attorney if necessary, to conduct a thorough investigation, which includes an assessment to determine whether a breach of unsecured protected health information under the HITECH regulation occurred and if so, what notifications are required. The Privacy or Security Officer should promptly complete its investigation within twenty (20) calendar days to ensure sufficient time for the preparation and coordination of notifications.
5. If the Privacy or Security Officer determines that there is no impermissible acquisition, access, use or disclosure of unsecured protected health information the investigating officer must note it in the comment section of the Breach Assessment Tool and Breach Reporting Form.
6. The investigating officer must maintain a copy of the Breach Assessment Tool and Breach Reporting Form and all documents related to the breach notification for six (6) years from the date it was created or the date it was last in effect, whichever is later.
7. The Privacy and Security Officers and departments that handle protected health information on behalf of the health care component must report breaches of five hundred (500) or more immediately to the Compliance Officer for reporting to the Department of Health and Human Services.
8. Each Health Care Component and departments that handle protected health information on behalf of the health care component must maintain a Breach Notification Log during a calendar year. The Breach Notification Log must be submitted to the Compliance Officer no later than December 31st of each year.

Notification

Individual Notification

1. Upon completion of the investigation of the breach, the investigating officer shall provide written notice immediately, not more than sixty (60) days for the date of discovery
   to the individual or:
   a. If the individual is deceased, to the next of kin or personal representative.
   b. If the individual is incapacitated/incompetent, to the personal representative.
   c. If the individual is a minor, to the parent or guardian.

   (See guidelines in the HIPAA Verification of Identity for Disclosure Policy prior to
   Releasing information someone other than the individual)
2. The written notification must be in plain language at an appropriate reading level and must meet Limited English Proficiency (LEP) requirements.
3. Written notification will be sent to the last known address of the individual or next of kin, or if specified by the individual, by electronic mail. The template letter in the Breach Notification Reporting Process must be used when sending written notification to an individual, personal representative, next of kin or parent.
4. If SCG determines the individual should be notified urgently of a breach because of possible imminent misuse of unsecured PHI, SCG will, in addition to providing notice as outlined above, contact the individual by telephone or other means, as appropriate.

Content of the Notification

The notification will include the following information relative to the breach:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. A description of the types of unsecured PHI that were involved in the breach, such as full name, social security number, date of birth, home address, account number, diagnosis code or disability code.
3. The steps the individual should take to protect themselves from potential harm resulting from the breach.
4. A brief description of what the covered entity is doing to investigate the breach, mitigate harm to the individual, and to protect against any further breaches.
5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

Substitute Notice

1. In the case where there is insufficient or out-of-date contact information that preclude
   written communication, a substitute notice will be provided accordingly:
   a. SCG will post a conspicuous notice for ninety (90) days on the homepage of our website that includes a toll-free number; or

b. SCG will provide notice in major print or broadcast media that serves Shelby County where an individual can learn whether or not their unsecured PHI is possibly included in the breach. A toll-free number will be included in the notice.

Media Notification

1. In the case where a single breach event affects more than five hundred (500) residents of Shelby County or the affected service area, the Compliance Officer will work with the Public Relations Department to develop a press release to submit to prominent media outlets in this area.

Health and Human Services (HHS) Notification

1. The Compliance Officer will provide electronic notice without unreasonable delay and in no case later than sixty (60) days from the breach discovery to the Secretary of the HHS if a single breach event was with respect to five hundred (500) or more individuals.

   The Compliance Officer shall submit a copy to the Chief Administrative Officer prior to submission to HHS.
2. The Compliance Officer will submit electronic notification to the HHS office breaches of less than 500 annually and no later than 60 days after the end of the calendar year.

   The Compliance Officer shall submit a copy to the Chief Administrative Officer prior to submission to HHS.

Delay of Notification for Law Enforcement Purposes

1. If a law enforcement official informs SCG that a notice or posting would impede a criminal investigation or cause damage to national security, SCG will delay the notice as follows:
   a. If the request is made in person, the requestor must present an agency identification badge, other official credentials, or other proof of government status;
   b. If the request is in writing, the request must be submitted on the appropriate government agency letterhead; or
   c. If the request is made via telephone, the SCG representative will note it in the file and request that the caller submit a written request. If a written request is not received in thirty (30) days, the SCG representative may release the breached information for notification to the individual and appropriate agencies.
   d. Documentation of the request must be noted in the file along with proof of identify of the government agency.

RESPONSIBLE PARTIES

Shelby County Government's Compliance Officer holds the chief responsibility of monitoring HIPAA compliance of each health care component. The administrative/management team of each health care component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

ENFORCEMENT

Employees violating this policy will be subject to the appropriate disciplinary process up to an including termination of employment.

REFERENCE

45 C.F.R. 164.404
164.406
164.408

Incident _____

SHELBY COUNTY GOVERNMENT
BREACH Assessment Tool

Privacy/Security Officer _____ Division _____

General Information
1. Name of the department that the breach occurred in. _____
2. Name of the individual discovering the breach _____
3. Name of administrative head the breach was reported to _____
4. Date breach occurred _____ Date of Discovery _____
5. Source or location where the breach occurred _____
6. Method of disclosure: Oral ___ Paper ____ Electronic _____
7. Number of Individuals Involved _____
8. Was the information accessed by an employee or business associate? _____
9. It further disclosed to another employee or business associate? _____
10. Name, title and department of employee or business associate that accessed the information or that the information was disclosed to _____ _____
11. If neither of persons mentioned in question nine accessed or disclosed such information, indicate the name of the person who did, if any known _____ _____

Source of Breach
__ Lost or stolen laptop, computer, flash drive, disk, etc. _____
__ Stolen password or credentials _____
__ Unauthorized access by an employee or contractor _____
__ Hacker __ Other (describe) _____
Is there any indication that the information was compromised (explain)? _____ _____

Type of Breach	
__ Name	__ Basic (age, sex, height, etc)
__ Address	__ Medical condition
__ Date of Birth	__ Treatments/procedures
__ Social Security Number	__ Mental Health
__ Drive license or identification care	__ Prescriptions
__ Financial information (credit or bank card)	__ Patient Chart
__ Health Insurance Card	__ Test Results
__ Other (describe) _____	

Brief Description of the Breach
_____ _____ _____ _____
Steps Being Taken to Investigate the Breach
_____ _____ _____ _____
Risk to Individual
__ Financial High ___ Medium ___ Low __ __ Reputation High ___ Medium ___ Low __
Describe the Steps Being Take to Mitigate Losses
__ Policies and Procedures _____ __ Technical Safeguards _____ __ Physical Safeguards _____ __ Other _____
Recommendations for the Individuals to Protect themselves Against the Breach
_____ _____ _____ _____
Date of Breach Notification
Individual _____ HHS _____ Media and name of media outlet _____ Substitute notice _____ If no notice has been sent, reason for delay _____ (all notifications should be attached to this form)
Comments
_____ _____ _____ _____

Incident _____

SHELBY COUNTY GOVERNMENT
BREACH Assessment Tool

Privacy/Security Officer _____ Division _____

General Information
1. Name of the department that the breach occurred in. _____
2. Name of the individual discovering the breach _____
3. Name of administrative head the breach was reported to _____
4. Date breach occurred _____ Date of Discovery _____
5. Source or location where the breach occurred _____
6. Method of disclosure: Oral ___ Paper ____ Electronic _____
7. Number of Individuals Involved _____
8. Was the information accessed by an employee or business associate? _____
9. It further disclosed to another employee or business associate? _____
10. Name, title and department of employee or business associate that accessed the information or that the information was disclosed to _____ _____
11. If neither of persons mentioned in question nine accessed or disclosed such information, indicate the name of the person who did, if any known _____ _____

Source of Breach
__ Lost or stolen laptop, computer, flash drive, disk, etc. _____
__ Stolen password or credentials _____
__ Unauthorized access by an employee or contractor _____
__ Hacker __ Other (describe) _____
Is there any indication that the information was compromised (explain)? _____ _____

Type of Breach	
__ Name	__ Basic (age, sex, height, etc)
__ Address	__ Medical condition
__ Date of Birth	__ Treatments/procedures
__ Social Security Number	__ Mental Health
__ Drive license or identification care	__ Prescriptions
__ Financial information (credit or bank card)	__ Patient Chart
__ Health Insurance Card	__ Test Results
__ Other (describe) _____	

Brief Description of the Breach
_____ _____ _____ _____
Steps Being Taken to Investigate the Breach
_____ _____ _____ _____
Risk to Individual
__ Financial High ___ Medium ___ Low __ __ Reputation High ___ Medium ___ Low __
Describe the Steps Being Take to Mitigate Losses
__ Policies and Procedures _____ __ Technical Safeguards _____ __ Physical Safeguards _____ __ Other _____
Recommendations for the Individuals to Protect themselves Against the Breach
_____ _____ _____ _____
Date of Breach Notification
Individual _____ HHS _____ Media and name of media outlet _____ Substitute notice _____ If no notice has been sent, reason for delay _____ (all notifications should be attached to this form)
Comments
_____ _____ _____ _____

Incident # _____

SHELBY COUNTY GOVERNMENT
BREACH Reporting Form

Privacy/Security Officer _____ Division _____

General Information
1. Name of the individual discovering the breach _____ 2. To whom was the breach reported? _____ _____ 3. Date breach occurred _____ Date of discovery _____ 4. If further disclosed, was it to an employee or business associate? _____ 5. If disclosed to an external source other than a business associate name entity or person the breach was disclosed to _____ 6. How many individuals were affected by the breach? _____ 7. Is there any indication that the information was compromised (explain)? _____ _____ _____

Type of Breach			
__ Loss	__ Improper Disposal	__ Hacker	__ Other
__ Theft	__ Unauthorized Access	__ IT Incident	__ Unknown

Location of the Breach			
__ Laptop	___ Desktop Computer	___ Electronic Medical Record	___ Paper
__ E-Mail	___ Network Server	___ Portable Electronic Device	___ Other

Protected Health Information Breached		
__ Name	___ Web Universal Resource Locator	___ Health Plan #
__ Address	___ Face Photographic Image	___ Medical Record #
__ Telephone	___ Certificates/ Licenses	___ E-Mail Address
__ Social Security #	___ Date of Birth/Age/Sec	___ Facsimile #
__ Credit/Card #	___ Other unique identifiers	___ License Plate #

Risk to Individual
___ Demographic ___ Financial ____ Clinical ____Reputation ___Other

Brief Description of the Breach
_____ _____ _____ _____

Steps Being Taken to Investigate the Breach

_____
_____
_____
_____

Safeguards in Place Prior to the Breach

___ Firewall	___ Physical Security
___ Packet Filtering (router-based)	___ Logical Access Control
___ Secure Brower Sessions	___ Anti-Virus Software
___ Strong Authentication	___ Intrusion Detection
___ Encrypted Wireless	___ Biometrics

Actions Taken in Response to the Breach

__ Policies and Procedures	__ Mitigation
__ Privacy and Security Safeguards	__ Sanctions
__ Employee Retraining	__ Other

Recommendations for the Individuals to Protect Themselves Against the Breach

_____
_____
_____
_____

Date of Breach Notification

Individual _____
HHS _____
Media and name of media outlet _____
Substitute notice _____
If no notice has been sent, reason for delay _____
(all notifications should be attached to this form)

Comments

_____
_____
_____

ATTESTATION

I attest, to the best of my knowledge, that the above information is accurate.

Name/Title _____ Date _____

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
Appropriate Workstation Use

Policy # (HS – 215)	**Supersedes Policy**
Approved By	**Effective Date**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date**

HIPAA Security Language – *Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.*

SCOPE/APPLICABILITY – This policy applies to all workforce and business associates who have been granted access to the Shelby County Health Department's workstations and information. This policy's scope includes all protected health information, as described in the Security Rule.

PURPOSE - To define acceptable workstation practices, to reduce the risk of unauthorized access to the Shelby County Health Department's information and to prevent loss, damage, and/or compromise of the Shelby County Health Department's assets and business activities.

POLICY - The Shelby County Health Department is committed to protecting the confidentiality and integrity of patient health information as required by law. Appropriate use of workstations entails appropriate and reasonable controls to prevent unauthorized access/use of the Shelby County Health Department's information and computer systems and to minimize business and patient care disruption. Departments that routinely handle protected health information are required to apply more stringent workstation controls due to the liability associated with the inappropriate disclosure of sensitive information.

All members of the Shelby County Health Department are required to be familiar with the contents of this policy and follow its guidance, as appropriate, when using computer equipment. Additionally, users who access the Shelby County Health Department's information and computer systems from remote locations must adhere to this policy.

PROCEDURES

User's Responsibilities

Users have an obligation to use workstations appropriately, effectively, and efficiently and for the Shelby County Health Department's business purposes only. Users must be aware that while performing job related responsibilities, sensitive and confidential patient health information may be displayed on the user's workstations. Therefore, users must exercise discretion and employ security measures equal to or exceeding that of written communication/documentation. These measures include:

1. Users must sign and uphold the terms of the Shelby County Health Department's Confidentiality Statement and Information System Users Access Notice.
2. Users must ensure that no one observes the entry of their password while logging into the system.
3. Users shall not log into the system under another user's password nor permit an individual to log into the computer under his/her password. Nor will any user enter data under another person's password.
4. Users should access patient health information on a need-to-know basis only.
5. Users should not disclose PHI to anyone that does not have an employee, client or business associate relationship with the Shelby County Health Department.
6. Users shall not leave an active workstation unsecured for prolonged periods of time, except where specifically authorized by the Shelby County Health Department in a controlled physical environment.
4. Users shall ensure that the workstation monitor is positioned so that they cannot be easily seen by anyone other than the user.
5. Users should not eat nor drink at the terminal to prevent damage to terminals due to spills.
6. Users must turn off their computer screens whenever leaving their desk for a period longer than one minute and less than fifteen minutes.
7. Users must sign off from the terminal before leaving for any time period beyond five minutes including the end of the day.

Department Heads/Manager Responsibilities

It is the responsibility of the Department Heads/Managers to ensure that employees receive appropriate workstation usage training.

Department Heads are also responsible for balancing the use of and controls over workstations in their physical environment to reasonably protect the Shelby County Health Department assets while supporting efficient workflow. For example, to prevent an unauthorized person from accessing data, workstations utilized by nurses in clinic hallways may be programmed to log off more quickly than the Shelby County Health Department's standards.

Technical Security Practices

The Shelby County Health Department has adopted the following technical safeguards to secure health information on the Shelby County Health Department's workstations.

1. An access control system approved by the Shelby County Health Department was installed on all workstations. In most cases this involved password-enabled screen-savers with a time-out-after- no-activity feature.
2. Prohibits unapproved workstations, workstation configurations, and computer systems or programs.
3. Allow only unique user login IDs and passwords.
4. Maintains accurate inventories of workstations, their location, and the department responsible for the workstation.
5. Conducts periodic security assessments of the Shelby County Health Department's workstation configuration and inventories to validate compliance with the Shelby County Health Department's acceptable workstation policies and practices.
6. Where applicable, backup of workstation data, programs, and computer systems must be performed on a regular basis to protect against business interruption.
7. Provide remote access to the Shelby County Health Department's computer systems and data for only approved users as evidenced by a properly approved and documented access request and appropriate and secure use of Protected Health Information.
8. Track and review remote workstation access audit trails on a periodic and timely basis. Notify the Information Security Officer of suspected compromised access or inappropriate accessed in a timely manner.

Prohibited Practices

The Shelby County Health Department will discipline employees in accordance with the Shelby County Health Department's HIPAA Sanctions Policy for inappropriate use of the workstation. Disciplinary actions will be taken for any of the unauthorized usage below, but not limited to the list below:

1. The use of programs or connection to the Internet that compromises the privacy of users and/or damages the integrity of the Shelby County Health Department's computer system, data, or programs.
2. Downloading or installing programs and data that is inappropriate or not specifically approved by the Shelby County Health Department.
3. The use of the Shelby County Health Department's workstations for personal gain.
4. Unauthorized attempts to break into any workstation.
5. Theft or access to electronic files without permission.
6. Sending or posting confidential files to unauthorized persons.
7. Refusing to cooperate with a reasonable security investigation.

Responsible Parties

Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each health care component. The administrative/management team of each health care component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers

are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement
Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment.

Reference
45 C.F.R. Sec. 164.310 (b)

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
Maintenance Records Policy

Policy # (HS – 216)	**Supersedes Policy**
Approved By	**Effective Date**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date**

HIPAA Privacy and Security Language – *Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks).*

SCOPE/APPLICABILITY – This policy requires the Shelby County Health Department to maintain records of the installation, modification and update, routine maintenance, and repair of the physical components of their building security systems. These components include doors, locks, walls, gates, alarms, alarm communication systems, window bars, fireproofing, sprinkler systems, smoke detectors, and equipment and devices used by security personnel (ie. televisions, monitors, camera systems, etc.).

This policy applies to all members of the Shelby County Health Department workforce, students, business associates, and any others who sign-off on repairs to any of the designated facility systems.

PURPOSE - The Shelby County Health Department has adopted this policy to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the privacy and security regulations, as well as, to fulfill our duty to protect the confidentiality and integrity of confidential protected health information as required by law, professional ethics, and accreditation requirements.

POLICY - The Shelby County Health Department will ensure compliance with this policy in order to provide reasonable assurance that repairs to the Shelby County Health Department facilities will not result in the negation of facility access protections put in place by the Shelby County Health Department.

1) Maintenance performed on doors, locks, walls, gates, alarms, alarm communication systems, window bars, fireproofing, sprinkler systems, smoke detectors and equipment, and devices used by security personnel (ie. televisions, monitors, camera systems, etc.) at the Shelby County Health Department locations is to be documented and submitted to the Shelby County Health Department Building Security Manager on the Maintenance Records Form. It is

the responsibility of the Supervisor or Building manager for the Shelby County Health Department location where the service is performed to submit the form as required.

2) The form must designate the system being maintained, changed, or updated, its location, the nature of the work performed, who performed the maintenance, including the company, and the signature of the Shelby County Health Department employee supervising or inspecting the maintenance.

3) All work performed on systems described in this policy must be inspected by a Shelby County Health Department employee prior to the submission of the Maintenance Records Form to insure that the system is fully functional.

4) Inspections must occur on the day of the repair or installation to ensure that the system will be operational during off hours (ie. nights or weekends).

5) Locations having compromised security systems must be reported to the Shelby County Health Department Building Security Manager by the Supervisor or Building Manager of the location prior to the location being left unattended for any period.

6) The Maintenance Records Forms are to be maintained for 6 years by the Shelby County Health Department Building Security Manager.

Enforcement
Employees, including students violating this policy will be subject to the appropriate disciplinary process up to an including termination of employment. Violation of this policy by the business associate may result in corrective action up to and including termination of the agreement. In some cases, civil and criminal penalties for misuse or misappropriation of health information and electronic media may occur. The violator should expect that the Shelby County Health Department shall provide information concerning the violation to appropriate law enforcement personnel and will cooperate with any law enforcement investigation or prosecution.

Reference
45 C.F.R. Sec. 164.310 (a)

Maintenance Records Form

Date: _____

Location/Address:

_____

System Affected and Location (ie. North entrance door lock, South gate hinge, etc.)**:**

Reason for Work (ie. break-in, structural damage, storm, etc.)**:**

Work Performed (ie. repair, installation, reconfiguration)**:**

Company or Department Performing Service:

Technician Performing Maintenance:

_____	_____	_____
(Name, Printed)	**(Date)**	**(Signature)**

SHELBY COUNTY HEALTH DEPARTMENT Employee Supervising Maintenance:

_____	_____	_____
(Name, Printed)	**(Date)**	**(Signature)**

Notes:

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
Disposal of Protected Health Information Policy

Policy # (HS – 217)	**Supersedes Policy**
Approved By	**Effective Date 04-20-05**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date**

HIPAA Security Language – *Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility as well as the movement of these items within the facility. Implement policies and procedures to address the final disposition of electronic protected health information and/or the hardware or electronic media on which it is stored.*

SCOPE/APPLICABILITY – This policy applies to all departments that store, maintain or access protected health information (PHI) for any purposes. This policy's scope includes all protected health information, as described in the HIPAA Privacy and Security Rules.

Key Definitions -

Patient Health Information Media: Any record of PHI, regardless of medium or characteristic that can be retrieved at any time. This includes all audiotapes, computerized data/hard disk drives, computer data/magnetic media, laser disks, microfilm/microfiche, PHI labeled devices/containers/equipment, paper records, video tapes, medical waste and other information recording media, regardless of physical form or characteristic, that are generated and/or received in connection with transacting patient care and business.

PURPOSE The Shelby County Health Department has a duty to protect the confidentiality and integrity of patient's medical information as required by law, professional ethics, and applicable state and federal law. Patient's health information may only be disposed of by means that assure that it will not be accidentally released to an outside party. Management must assure that appropriate means of disposal are reasonably available and operational. The purpose of this policy is to define the guidelines and procedures that must be followed when disposing of information containing PHI.

POLICY - It is the policy of the Shelby County Health Department to ensure the privacy and security of PHI in its maintenance and retention, and the re-use and permanent destruction/disposal of such media. All destruction/disposal of patient health information media will be done in accordance with federal and state law, the Shelby County Health Department's Retention of Patient Medical Records and Disposal of Protected Health Information Policy. The Shelby County Health Department's policy for destroying medical and patient financial records are as follows:

- Records will only be destroyed in the ordinary course of business.
- No entire record shall be destroyed on an individual basis.
- Destruction of records involved in open investigations, or pending or anticipated litigation will be suspended until such matter is resolved.
- Paper records and patient data stored on electronic/magnetic media, which are not being used for active patient care or payment processes, may be archived in a secured environment until the retention requirements have been met.
- Clinics and departments may determine the criteria for inactive record status in their areas, based on need for the records and available storage space.
- Records that have satisfied the period of retention will be destroyed/disposed of in a manner that ensures the patient's information cannot be recovered or reconstructed.

PROCEDURE
Destruction of Convenience Copies and Original Document (Day-To-Day Destruction)

1. The Shelby County Health Department shall provide users with access to sufficient shredders for proper disposal of confidential printouts containing PHI.
2. It is the user's responsibility to ensure that the document has been properly secured in a publicly accessible shredder located within the facility. And it is the supervisor's responsibility to ensure that their employees are adhering to the policy.

Disposal of Records Containing PHI

1. A record of all patient's health information media destruction/disposal will be made and retained permanently by the Shelby County Health Department. Permanent retention is required because the records of destruction/disposal may become necessary to demonstrate that the client information records were destroyed/disposed of in the regular course of business. Records of destruction/disposal should include:
    A. Date of destruction/disposal.
    B. Method of destruction/disposal.
    C. Description of the destroyed/disposed record series or medium.
    D. Inclusive dates covered.
    E. A statement that the patient information records were destroyed/disposed of in the normal course of business.
    F. The signature of the individual destroying/disposing of the PHI and the signature of a notary.

2. If hardcopy PHI (paper, microfilm, microfiche, etc.) cannot be shredded, it must be incinerated or otherwise disposed of in a manner allowed under state law.
3. If the record destruction is performed by the Shelby County Health Department or Shelby County Government Archive's Department, the Shelby County Health Department personnel must complete the Record Disposal Request Form. This form must be signed by the Department Head, and confirms the appropriate destruction of the data.
4. Records may not be destroyed without the approved signatures of Tennessee Public Records Commission chairman and secretary affixed to the Record Disposal Form.

Disposal of PHI by Business Associates

1. Contracts between Shelby County Health Department and its business associates will provide that, upon termination of the contract, the business associate will return or destroy/dispose all patient health information. The destruction of PHI by the Business Associate will be documented in writing and sent to the Shelby County Health Department.
    A. Date of destruction/disposal.
    B. Method of destruction/disposal.
    C. Description of the destroyed/disposed record series or medium.
    D. Inclusive dates covered.
    E. A statement that the patient information records were destroyed/disposed of in the normal course of business.
    F. The signature of the individual destroying/disposing of the PHI and the signature of a notary.

2. If such return or destruction/disposal is not feasible, the contract will limit the use and disclosure of the information to the purposes that prevent its return or destruction/disposal.

Disposal of PHI that has been Outsourced

1. If destruction/disposal services are contracted, the business associate agreement must provide that the Shelby County Health Department's business associate must adhere to the permitted and required uses and disclosures of information by the business associate as set forth in the federal and state law (outlined in Health Care Component's HIPAA Business Associate Agreement/Contract) and include the following elements:
    A. Specify the method of destruction/disposal.
    B. Specify the time that will elapse between acquisition and destruction/disposal of data/media.
    C. Establish safeguards against breaches in confidentiality.
    D. Indemnify Shelby County Health Department from loss due to unauthorized disclosure.
    E. Require that the business associate maintain liability insurance in specified amounts at all times the contract is in effect.

F. Provide proof of destruction/disposal.

Disposal of Electronic Media

Department Managers are responsible to contact the Information Technology Department when redeploying any electronic storage media/device with Shelby County Health Department to ensure proper removal of information, including PHI from such device.

PHI media should be destroyed/disposed of using a method that ensures the PHI could not be recovered or reconstructed. Appropriate methods for destroying/disposing of media are outlined in the following table:

Medium	Recommendation
Audiotapes	Recycling by recording over the original user, or pulverize the tape and cassette.
Computerized Data/Hard Disk drives	Overwrite all data with a series of characters after reformatting the disk. Overwriting should include any back-up tapes or professional purging by a certified, licensed, and bonded vendor.
Computer Data/Magnetic Media	Overwrite all data with a series of characters after reformatting the tape, including back-up tapes, and/or magnetically degauss.
Laser Disks	(Write-Once-Read-Many) applications cannot be altered or reused, making pulverization an appropriate means of permanent destruction/disposal.
Microfilm/Microfiche	Shred or pulverize only.
PHI Labeled Devices, Containers, Equipment, Etc.	Reasonable steps should be taken to destroy or de-identify any PHI information prior to disposal of this medium. Remove and destroy all PHI on the label or incinerate the devices, container, etc., if removal or destruction of the label is impossible.
Paper Records	Paper records should be destroyed/disposed of in a manner that leaves no possibility for reconstruction of information. Appropriate methods for destroying/disposing of paper records include shredding pulverizing or electronically purged or place in locked or otherwise secure storage for controlled shredding/destruction later.
Videotapes	Methods for destroying/disposing of

	videotapes include recycling (tape over) or pulverizing.
Medical Waste	Waste must be placed in regulated medical waste bins. All regulated medical waste trash is incinerated using secure methods.

Re-use of Storage Devices or Removable Media

1. Any equipment or storage media that contains PHI will be erased by appropriate means or destroyed by the Security Officer or his/her appointed designee.
   A. Prior to making storage devices and removable media available for reuse, care must be taken to ensure that the device or media does not contain PHI.
   B. If the device or media contains the only copy of PHI that is required or needed, a retrievable copy of the PHI must be made prior to reuse.
   C. If the device or media contains PHI that is not required or needed, and are not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to reuse. See the "Disposal of Electronic Media" section above for data destruction recommendations.
   D. If using removable media for the purpose of system backups and disaster recovery and the aforementioned removable media is stored and transported in a secured environment, the use of a data destruction tool between uses is not necessary.
2. The Shelby County Health Department's Information Security Officer is responsible for the removal of all the Shelby County Health Department's information, including PHI, resident on any electronic storage media/device prior to transferring, re-use, donation or a sale of such devices.
3. Upon completion of any transaction mentioned in item (2) of this section, the Information Security Officer will account for this transaction on the Electronic Disposition Form. The fully executed Electronic Disposition Form will be kept on file in the Information Technologies department.

The Security Officer, based on current technology, accepted practices, and availability of timely and cost-effective destruction/disposal services, should reassess methods of destruction/disposal annually.

Shelby County Health Department will maintain documentation of the record destruction for the life of the institution.

Responsible Parties

Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each health care component. The administrative/management team of each health care component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement
Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment.

Reference
45 C.F.R. Sec. 164.310 (d)(2)

Shelby County Health Department
Information Technologies
Electronic Media Disposition Form

Start Date _____-_____-_____ End Date _____-_____-_____

Requestor	Requestor's Initials	Department	Phone Number	Media Description	IT Employee Initials	Date
						_____-_____-_____
						_____-_____-_____
						_____-_____-_____
						_____-_____-_____
						_____-_____-_____
						_____-_____-_____
						_____-_____-_____
						_____-_____-_____

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
Workstation Security Policy

Policy # (HS – 218)	**Supersedes Policy**
Approved By	**Effective Date**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date**

HIPAA Security Language – *Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.*

SCOPE/APPLICABILITY – All persons with access to the equipment and services provided by the Shelby County Health Department have a responsibility to assure protection from misuse and abuse.

PURPOSE: Security of electronic equipment and products is critical to the operation of the Shelby County Health Department. The purpose of this policy is to establish guidelines for the physical security of the Shelby County Health Department's electronic files.

POLICY - The Shelby County Health Department is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and regulations. Accordingly, the Shelby County Health Department's officers, employees and agents will preserve the integrity and the confidentiality of individually identifiable health information pertaining to each patient.

Servers

1. Computer servers will be located in areas where access is limited to authorized persons only. Areas in which unattended servers are located will be secured with locked doors.
2. The environment for computer equipment will contain humidity and temperature controls.
3. All servers will be protected from power surges with an appropriate uninterruptible power source. That power source will provide enough capacity to either safety shutdown the equipment or switch to an alternative power source such as a generator in the event of a loss of power.
4. Servers that are connected to the Internet must be protected by a firewall.
5. A procedure for creating and maintaining backup media, both on-site and off-site shall be in place and followed.

6. All system and application logs will be maintained in a form that cannot readily be viewed by unauthorized persons, and backed-up on a periodic basis. All logs will be audited on a periodic basis.
7. Intrusion detection and network monitoring are both on a 24 x 7 basis and all attempted unauthorized access to the network should be logged and reported.

Technical Security Practices
The Shelby County Health Department has adopted the following technical safeguards to secure health information on Shelby County Health Department workstations.

1. An access control system approved by the Shelby County Health Department is installed on all workstations. In most cases this involved password-enabled screen-savers with a time-out-after-no-activity feature.
2. Unapproved workstations, workstation configurations, computer systems, or programs are prohibited.
3. Only unique user login IDs and passwords are allowed.
4. After three failed attempts to log on, the system will refuse access to the account until it is reset.
5. Maintains accurate inventories of workstations, their location, and the department responsible for the workstation.
6. Conducts periodic security assessments of the Shelby County Health Department's workstation configuration and inventories to validate compliance with the Shelby County Health Department acceptable workstation policies and practices.
7. Provide remote access to Shelby County Health Department computer systems and data only for approved users with properly approved and documented access request forms on file.
8. The security Officer will re-evaluate security procedures annually to determine if changes in technology, equipment, applicable regulation, or other factors may affect the security of EPHI held by Health Care Component.

Responsible Parties
Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each health care component. The administrative/management team of each health care component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement
Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment.

Reference
45 C.F.R. Sec. 164.

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY
TRANSMITTAL OF PHI BY FACSIMILE

Policy # (HS – 219)	**Supersedes Policy**
Approved By	**Effective Date**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date**

SCOPE/APPLICABILITY – This policy applies to all the Shelby County Health Department's workforce members as defined by the HIPAA Privacy Rule. This policy's scope includes all protected health information, as described in the HIPAA Privacy and Security Rules.

PURPOSE - The HIPAA Privacy Regulations require that covered entities implement appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. The purpose of this policy is to provide instructions to all Shelby County Health Department departments and workforce members regarding transmitting PHI by facsimile and the measures necessary to maintain an adequate level of security from such information.

POLICY

The Shelby County Health Department requires that facsimiles containing PHI only be received or sent to the departmental specific fax machines and not to systems that have general access. In cases, where PHI is received from an external source on a non-departmental specific facsimile machine the receiving department shall notify The Shelby County Health Department's Privacy Officer of the source of such information. The department shall communicate the approved facsimile number to the external entity and record such actions. Should PHI be disclosed by facsimile to an inappropriate party, the Shelby County Health Department shall, to the extent possible, remedy such disclosures. All facsimile documents sent by the Shelby County Health Department workforce members shall contain the following statement:

THIS FAX IS INTENDED FOR THE INDIVIDUAL/INDIVIDUALS OR ENTITY/ENTITIES NAMED ABOVE AND MAY BE COVERED BY COPYRIGHTS, BUSINESS PARTNER CONFIDENTIALTIY AGREEMENTS, NONDISCLOSURES OR OTHER LEGALLY BINDING INSTRUCTMENTS. DO NOT READ, COPY, USE OR DISCLOSE THE CONTENTS OF THIS COMMUNICATION TO OTHERS. IMMEDIATELY NOTIFY THE SENDER BY REPLY FAX, DESTROY ALL HARD COPIES AND DELETE THIS DOCUMENT FROM ALL SYSTEMS. THANK YOU!

PROCEDURE

1. All Shelby County Health Department departments are required to use the approved pre-printed facsimile cover sheet form that includes the Shelby County Health Department's confidentiality statement for messages containing PHI.

2. Each department should pre-program facsimile machines with frequently dialed numbers to prevent misdialing errors.

3.The department shall periodically test the programmed numbers for accuracy and authorization to receive PHI (i.e., send a cover sheet and verify by phone or in person that it was received).

4. Facsimiles sent to unknown or unfamiliar locations should be phone-verified before any PHI is transmitted. The cover sheet should be sent alone and the workforce member should call to verify that the intended and authorized person received it or is standing by to receive the PHI documents that will follow.

5. The Shelby County Health Department workforce will limit the transmitting of PHI to the minimum necessary needed for the requestor to accomplish the intended purpose.

6. In the case where data-containing PHI is disclosed by facsimile to an inappropriate party, the following procedure shall be followed:

A. The receiving party shall be contacted by telephone immediately and requested to destroy the facsimile without reading.
B. The name of the company, the person contacted, the date and time shall be recorded as well as any comments made by the person receiving such calls.
C. A facsimile shall also be sent to the receiving party containing the same instructions as detailed for the phone call requesting a return facsimile message indicating that the requested action was taken.
D. The cause of the inappropriate disclosure shall be determined and reported to the Shelby County Health Department's Privacy Officer.
E. Methods to prevent a re-occurrence of the disclosure shall be formulated and put into place.
F. Any additional actions prescribed by regulations shall be performed.

7. The Shelby County Health Department workforce faxing PHI for non-treatment, payment or health care operations (TPO) purposes without a signed authorization must account for the non – TPO disclosure. Please refer to the Shelby County Health Department's Accounting of Disclosure Policy.

Responsible Parties

Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each health care component. The administrative/management team of the Shelby County Health Department must ensure that sections under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement
Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment.

Reference
45 C.F.R.

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
Acceptable Encryption Policy

Policy # (HS – 221)	**Supersedes Policy**
Approved By	**Effective Date 04-20-05**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date 05-27-10**

HIPAA Security Language – *Implement a mechanism to encrypt and decrypt electronic protected health information. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.*

SCOPE/APPLICABILITY – This policy applies to all departments and workforce members regarding SHELBY COUNTY HEALTH DEPARTMENT authorized encryption technologies for use with data containing PHI. This policy's scope defines the rules necessary to maintain the protection of PHI when communicating such data across networks that include or may include public infrastructure or otherwise insecure segments.

Definition
Proprietary Encryption – An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Symmetric Cryptosystem – A method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem – A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

PURPOSE - The HIPAA Privacy Regulations require that covered entities implement appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. The purpose of this policy is to provide guidance and limit the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively and approved for use by the Shelby County Health Department. Additionally, this policy provides direction to ensure that the requirements of HIPAA and Centers for Medicare and Medicaid Services are followed.

POLICY - It is the policy of the Shelby County Health Department to use only proven, standard algorithms/ methods such as Triple-DES, RSA, RC5, IP/Sec, PKI, Kerberos and IDEA as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Pretty Good Privacy (PGP) uses a combination of IDEA and RSA, while OpenSSL may use RSA, RC5 or other encryption algorithms. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength.

All PHI transmitted from the Shelby County Health Department's communication network to non- Shelby County and/or external Internet destination must be encrypted.

The Shelby County Health Department's key length requirements will be reviewed annually and upgraded as technology requires.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by the appropriate Shelby County Health Department departments and approved by the Executive Director and HIPAA Technical Security Subcommittee. Additionally, any wireless technologies implemented must meet all requirements established by this policy.

Responsible Parties

Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each health care component. The administrative/management team of each health care component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement

Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment.

Reference

C. F. R. Sec. 164.312 (a)(2)(iv) & (e)(2)(ii)

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
Transmitting Protected Health Information by E-Mail

Policy # (HS – 222)	**Supersedes Policy**
Approved By	**Effective Date 04-20-05**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date**

HIPAA Security Language – *Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communication network.*

SCOPE/APPLICABILITY – This policy applies to all usage of electronic mail systems within the Shelby County Health Department whether the mail originated from or is forwarded in a Shelby County Health Department computer or network. This policy's scope includes all protected health information, as described in the HIPAA Privacy and Security Rules.

PURPOSE - The HIPAA Privacy Regulations require that covered entities implement appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. The purpose of this policy is to provide instructions to all the Shelby County Health Department departments and workforce members regarding the use of e-mail with respect to PHI and the measures necessary to maintain an adequate level of security from such information.

POLICY - The Shelby County Health Department requires its workforce members to exercise extreme caution when sending e-mail to or receiving from an external network. Prior approval must be obtained from the Shelby County Health Department's Executive Director or Privacy Officer before any personnel can transfer data containing PHI to an external destination. External e-mail communication will be handled accordingly:

- E-mail must meet all requirements of the Shelby County Health Department's Acceptable Encryption Policy.
- The Minimum Necessary Rule must be applied to all e-mail correspondence that contains PHI. Please see the Shelby County Health Department's Minimum Necessary Policy.
- Editorial comments, including opinions, assumptions, and speculations should be excluded from all e-mail correspondence.

- Unencrypted e-mail that contains PHI, received from external sources should be reported to the Shelby County Health Department's Privacy Officer.
- The Privacy Officer will communicate the approved secure methods of data transfer to the external entity.
- Should PHI be disclosed via an e-mail to an inappropriate party by the Shelby County Health Department, it shall follow the procedures outlined under item 3 and below, to the extent possible, to resolve such disclosures.

The following statement shall be appended as a footer to all e-mail that contains PHI:

NOTE: The information in this message is confidential and may be legally privileged. It is intended solely for the addressee. Access to this message by anyone else is unauthorized. If you are not the intended recipient, any disclosure, copying, or distribution of the message, or any action or omission taken by you in reliance on it, is prohibited and may be unlawful. Please delete this e-mail and immediately contact the sender if you have received this message in error.
Thank you.

The removal of E-Mail containing Protected Health Information from the Shelby County Health Department is prohibited.

PROCEDURE

1. Communication by e-mail between clinicians and patients may be used only if the patient has signed an authorization.
   A. Clinically relevant e-mail messages must be printed in full, including any responses and included in the patient's medical record.
2. Communication by e-mail between and among clinicians and support staff may be used for the following purposes only:
   - Requesting Consultations
   - Making Referrals
   - Prescription Refills
   - Billing Inquires
3. E-mail containing PHI may not be (auto) forwarded to any external e-mail address including but not limited to, personal and commercial e-mail accounts such as AOL, Yahoo, Road Runner, etc.
4. When replying to e-mail containing PHI from external addresses the response may not contain PHI.
5. No distribution list may be used for e-mail that contains PHI

6. In the case where data containing PHI is disclosed by e-mail to an inappropriate party, whether encrypted or not, the following procedure shall be followed:
   A. An e-mail shall be sent to the receiving party immediately requesting the receiver to delete the e-mail prior to opening. If the e-mail has been opened, the receiving party should be requested to delete the e-mail and to maintain the confidentiality of the information divulged.

B. The Shelby County Health Department personnel shall follow up with a telephone to the receiving party to confirm that the requested action was taken.
C. The name of the company, the person contacted, the date and time of the contact shall be recorded as well as any comments made by the receiving party of such calls.
D. The cause of the inappropriate disclosure shall be determined and reported to the Shelby County Health Department's Privacy Officer.
E. Methods to prevent a re-occurrence of the disclosure shall be formulated and put into place.
F. Any additional actions prescribed by regulations shall be performed.

Responsible Parties
Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each health care component. The administrative/management team of each health care component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement
Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment.

Reference
45 C.F.R. Sec. 164.512 (e)(1)

SHELBY COUNTY GOVERNMENT
Shelby County Health Department

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
Audit Controls Policy

Policy # (HS – 223)	**Supersedes Policy**
Approved By	**Effective Date**
HSC _____ Date ____	**Review Date**
ED _____ Date ____	**Revision Date**

HIPAA Security Language – *Implement hardware, software, and/or procedural mechanisms that record and examine activity on information systems that contain or use electronic protected health information*

SCOPE/APPLICABILITY – The scope of this Policy covers the hardware, software and/or procedural mechanisms that will be implemented by the Shelby County Health Department Departments to record and examine activity on information systems that contain or use EPHI.

PURPOSE - The Shelby County Health Department is committed to conducting business in compliance with all applicable laws, regulations and Shelby County Health Department policies. The Shelby County Health Department has adopted this policy to set forth the internal audit procedures for security of EPHI that each Department must implement.

POLICY - The Shelby County Health Department is a covered entity under the Health Insurance Portability and Accountability act of 1996 (HIPAA). Accordingly, Shelby County Health Department officers, employees, and agents shall preserve the integrity and the confidentiality of individually identifiable health information pertaining to each patient.

1. Audit Control Mechanisms

All Shelby County Health Department systems containing medium and high risk EPHI must utilize a mechanism to log and store system activity.

a. Each system's audit log must include, at a minimum, User ID, file accessed, and/or file deleted. Audit logs may include system and application log-in reports, activity reports, exception reports or other mechanisms to document and manage system and application activity.
b. System audit logs must be reviewed on a regular basis. (See the Shelby County Health Department's Risk Management and System Activity Review Policies).
c. Implementation of an audit control mechanism for systems containing low risk EPHI is not required.

2. Audit Control and Review Plan

An Audit Control and Review Plan must be developed for all the Shelby County Health Department's systems housing ePHI. These plans must be approved by the HIPAA Security Office. If the Shelby County Health Department's ePHI inventory changes, the Audit Control and Review Plan must be reevaluated and resubmitted to the HIPAA Technical Security Subcommittee.

The plan must include:

- Systems and applications to be logged
- Information to be logged for each system
- Log-in reports for each system
- Procedures to review all audit logs and activity reports

Responsible Parties

Shelby County Government's Health Policy Coordinator holds the chief responsibility of monitoring HIPAA compliance of each Health Care Component. The administrative/management team of each Health Care Component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

Enforcement

Employees violating this policy will be subject to the appropriate disciplinary process up to and including termination of employment. Additionally, temporaries and volunteers who do not attend training and fail to furnish document of training will not be allowed to furnish services to the Shelby County Health Department.

Reference

C. F. R. Sec 164.